The bridge to possible

Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 3 応用設定編

Rev 2.0

August 2022

シスコシステムズ合同会社

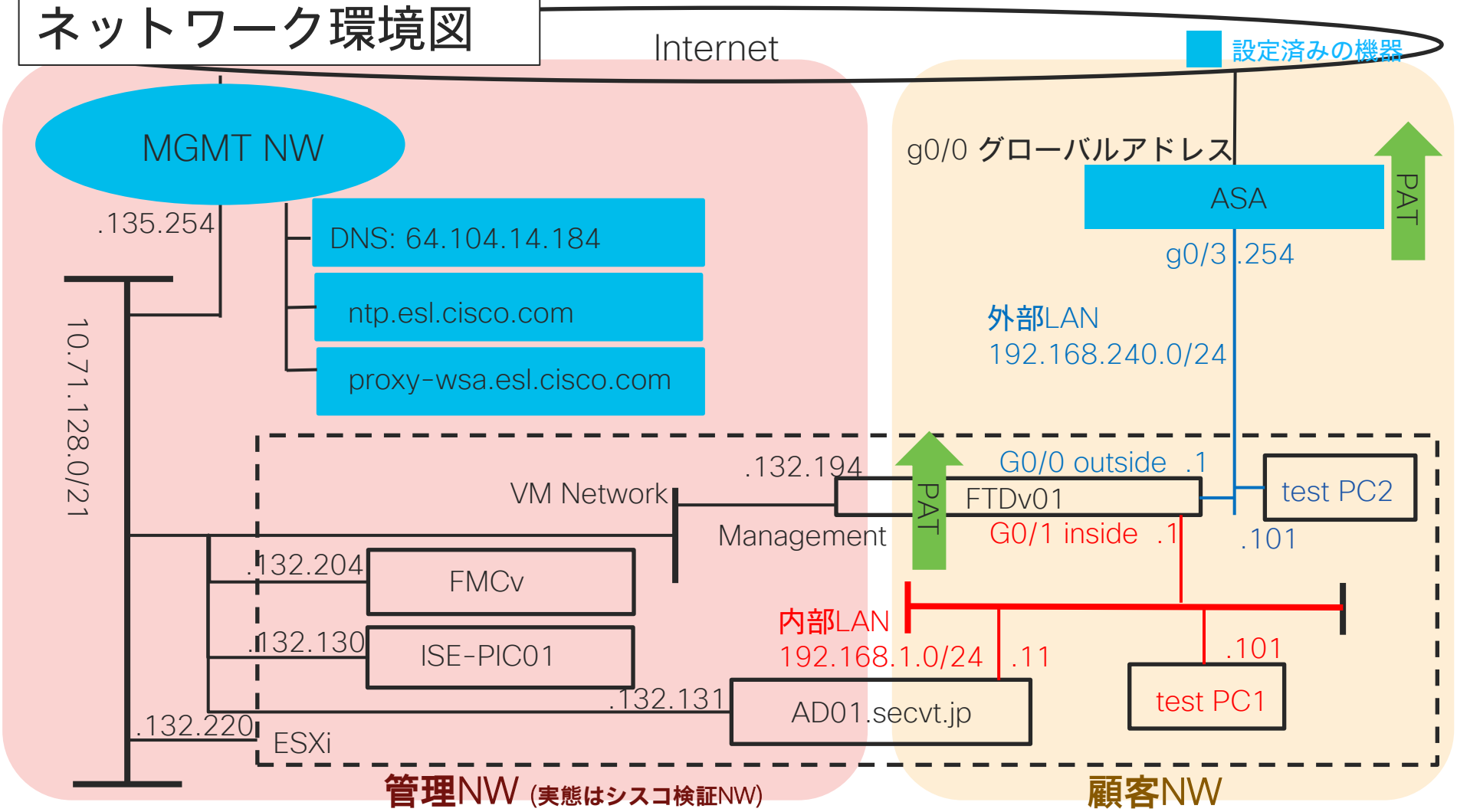
はじめに

- 本ガイドは、Version 7.0 の Firewall Management Center (以下、FMC) 管理の Firewall Threat Defense (以下、FTD) の初期セットアップ方法を解説しております。
- 本ガイドは、FTD と FMC の仮想版を使って、評価作業を開始できることをゴールとしております。
- 本ガイドは、4部作の Vol. 3 に相当します。

内容に関する保証について

- 本ガイドは、2022年8月現在の情報に基づいており、FTD & FMC のソフトウェアは 7.0.x を、ハイパーバイザは VMware ESXi 6.5 を利用しております。
- 本ガイドに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。
- シスコは、本ガイドに関して、その正確性又は完全性について一切の責任を負わないこととします。
- シスコは、本ガイドが十分な品質を有すること、特定の目的に対する適合性を有すること、又は第三者の知的財産権、プライバシー権等その他の一切の権利に対する侵害がないことを、明示にも黙示にも表明又は保証しません。

ネットワーク環境図


Internet
設定済みの機器
MGMT NW
.135.254
10.71.128.0/21
DNS: 64.104.14.184
ntp.esl.cisco.com
proxy-wsa.esl.cisco.com
g0/0 グローバルアドレス
ASA
PAT
g0/3 .254
外部LAN
192.168.240.0/24
.132.194
VM Network
Management
PAT
FTDv01
G0/0 outside .1
G0/1 inside .1
test PC2
.101
.132.204
FMCv
.132.130
ISE-PIC01
内部LAN
192.168.1.0/24
.11
.101
test PC1
.132.131
AD01.secvt.jp
.132.220
ESXi
管理NW (実態はシスコ検証NW)
顧客NW

当ガイド (Vol. 3) のシナリオ

- SSL Policy にて内部から外部への通信を復号し、セキュリティ検査を適用する。
- ISE-PIC を導入し、Active Directory と連携することで、AD ログオン時のユーザによってセキュリティポリシーを使い分ける Identity Firewall を利用する。
- FTDv にて AnyConnect を使ったリモートアクセス VPN を接続を提供し、さらに VPN 接続時にもセキュリティポリシーを適用する。
- FTDv, FMCv のバックアップを取得し、有事の際のリストアを検証する。

注意事項

- 製品名称が更新されているが、ソフトウェア名称は旧製品のままで公開されている
- 新名称 ←→ 旧名称
  - Firewall Management Center ←→ Firepower Management Center
  - Firewall Threat Defense ←→ Firepower Threat Defense

Vol.1 (初期インストール編) の目次

1. FMC と FTD のインストール
   1-1. FMCv の初期インストール
   1-2. FTDv の初期インストール
   1-3. (Option) FPR4100/9300 シリーズの初期インストール
   1-4. (Option) FPR1000/2100 シリーズの初期インストール
2. FTD と FMC その他初期設定
3. シグネチャ及び各種 DB の更新
4. スマートライセンスの適用
5. FMC と FTD の Upgrade / Patch インストール

Vol. 2 (基本セキュリティポリシー設定編) の目次

6. Routed Firewall, NAT および Network Discovery の設定
7. Prefilter の設定
8. Intrusion Policy の設定 (Snort3)
9. Malware & File Policy の設定
10. Access Control Policy の設定

Vol. 3 (応用設定編:当ガイド) の目次

11. TLS Decryptionの設定
12. IDFW の設定
13. AnyConnect VPN 接続の設定
14. バックアップの設定とリストアの方法

Vol. 4 (管理・監視・冗長構成編) の目次

15. FMC API の利用例
16. システム監視
17. Syslog・レポート・アラートの設定
18. SAL SaaS, SecureX 連携の設定
19. 設定ロールバック
20. FTD High Availability の設定
21. FMC High Availability の設定

11. TLS Decryption の設定

TLS 復号アクセラレーション

- SSL/TLS 暗号通信を復号してインスペクションを行う機能
  - inbound inline (L1), transparent (L2), routed (L3)

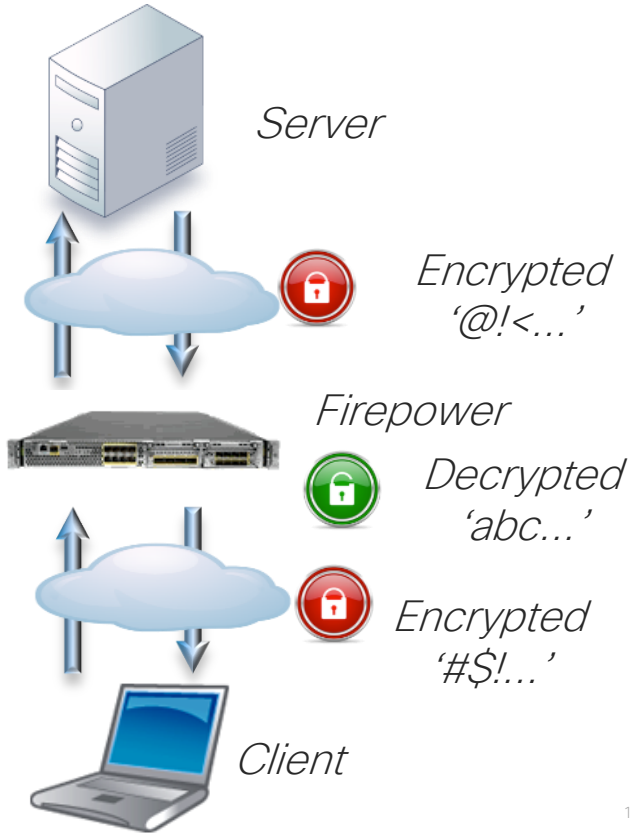
    → Decrypt – Known Key 設定を利用

    → 主に不特定多数の端末から自身が管理している公開サーバへの通信を復号。 IPS 機能と併用される場合が多い
  - outbound inline (L1), transparent (L2), routed (L3)

    → Decrypt – Resign 設定を利用

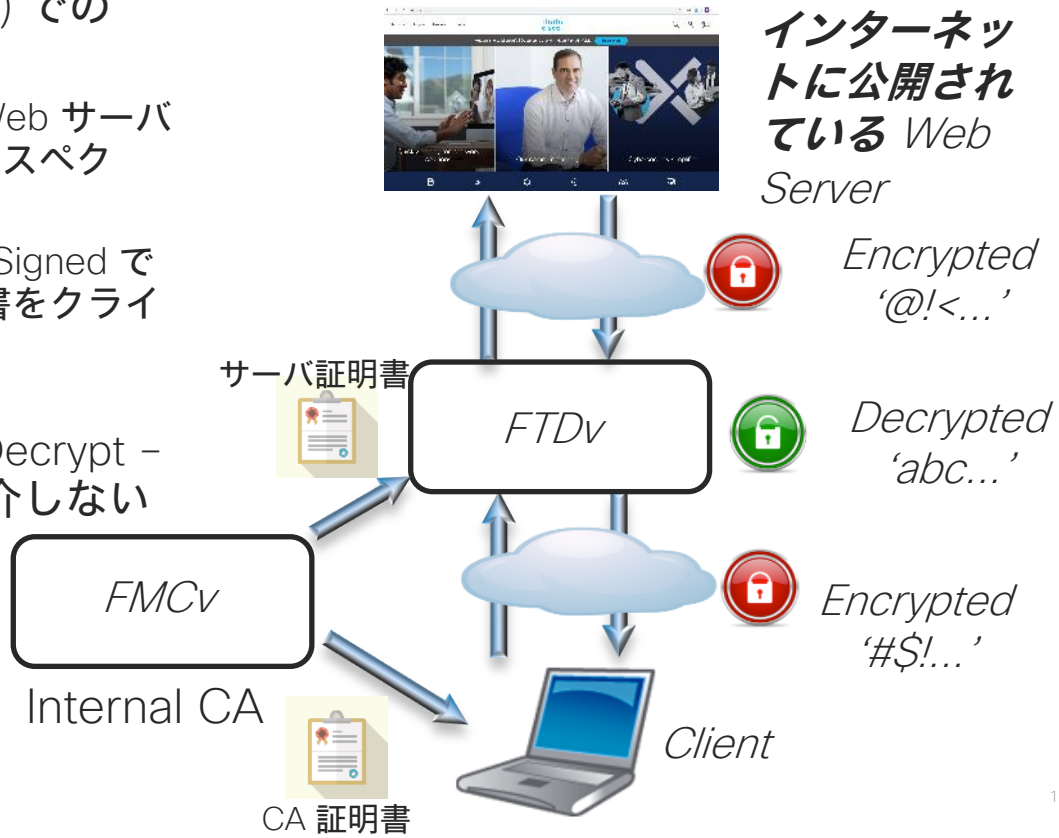
    → 主に自身が管理しているネットワーク内から不特定多数の公開サーバへの通信を復号。 NGFW 機能と併用される場合が多い
- Firepower 1K,3K,4k,9k はハードウェア処理による高速処理が可能。詳しくはデータシート参照
- 復号・再暗号化や仲介管理が、負荷や遅延の原因となるため、必要な通信のみ Decrypt するなどメリハリ付けを
  (運用例：定期バックアップや 信頼サイトは Decrypt しない)
- Inline TAP, passive interface では未サポート

FTD は MITM (Man In The Middle) の形で通信を復号し、インスペクション後にまた通信
を暗号化する

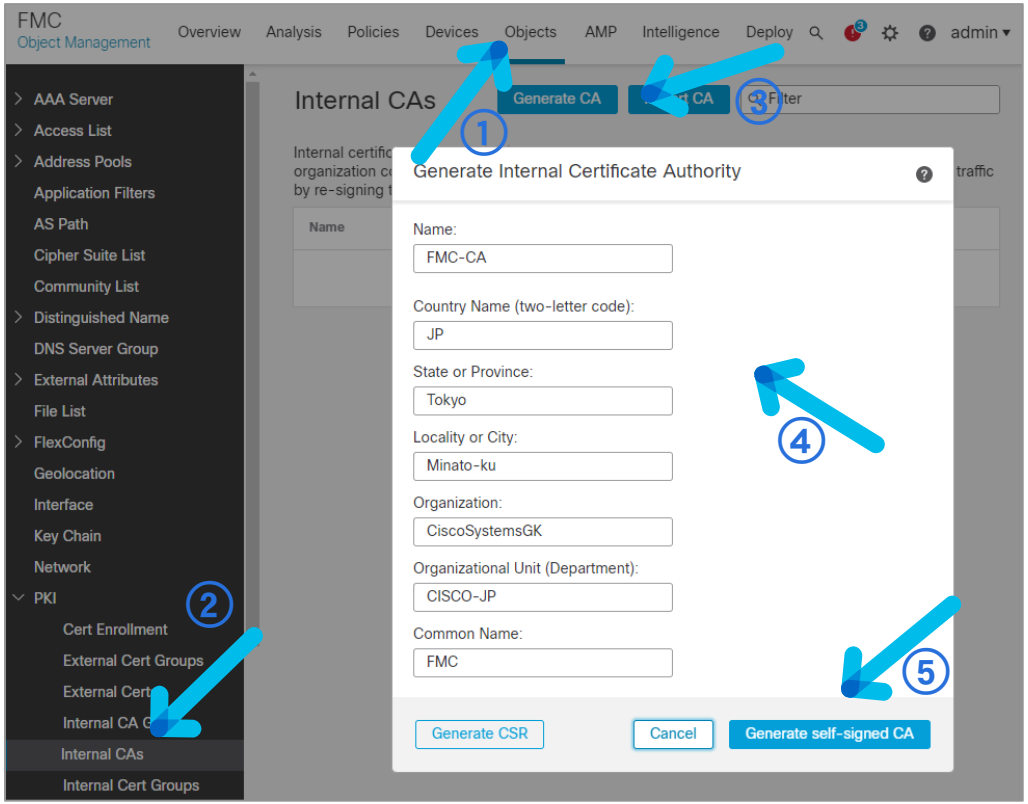


このガイドでのシナリオ

- Outbound (i.e. Decrypt – Resign) での TLS 復号をを紹介
  - インターネットに公開されている Web サーバにアクセスする際に、FTD でのインスペクションを行う
  - 簡素化のため、Internal CA を Self-Signed で FMC にて立ち上げ、その CA 証明書をクライアントにインストールする
- このガイドでは、Inbound (i.e. Decrypt – Known Key) での TLS 復号は紹介しない



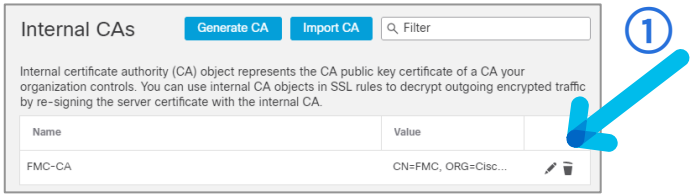
ステップ1: FMC での Internal CA 作成

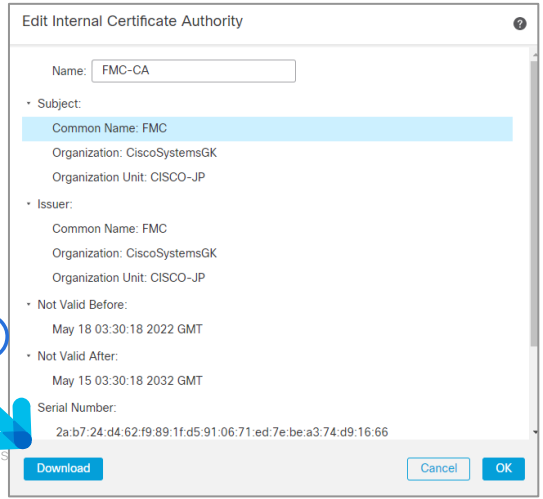


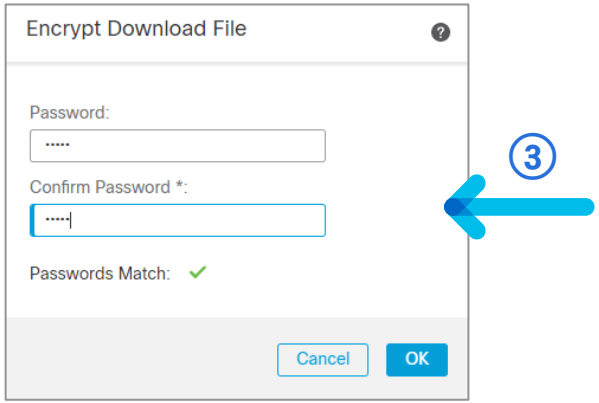
① FMC にて Objects > Object Management を選択
② PKI > Internal CAs を選択
③ Generate CA をクリック
④ Internal CA に必要なパラメータを埋める
⑤ Generate self-signed CA をクリック
⑥ Internal CA が作成される

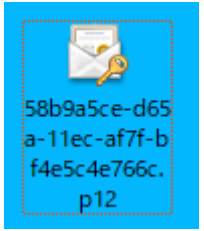
ステップ2-1: Internal CA の証明書を入手

テスト PC は FMC の Internal CA を信頼する必要があるため、Internal CA の証明書をテスト PC の「信頼されたルート証明機関」にインポートする。 まずは Internal CA の PKCS #12 形式のファイルを入手する







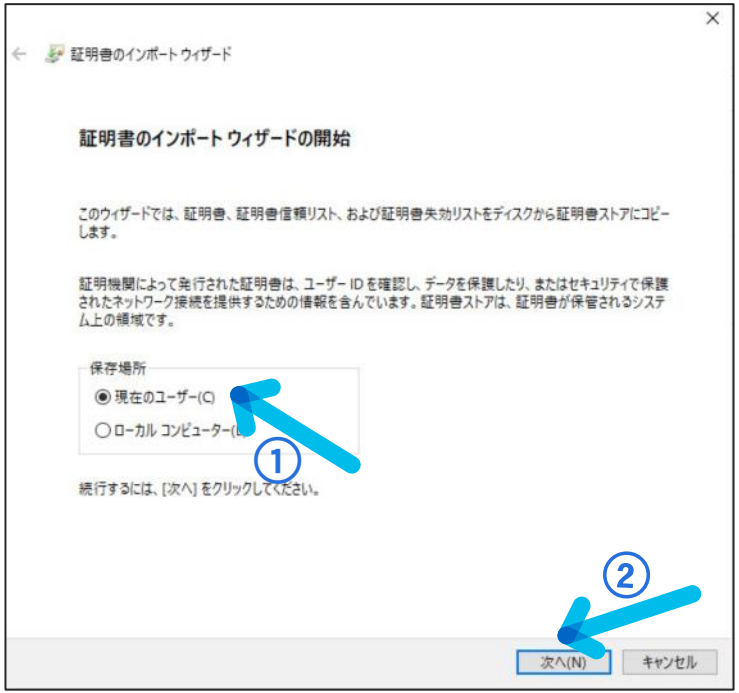


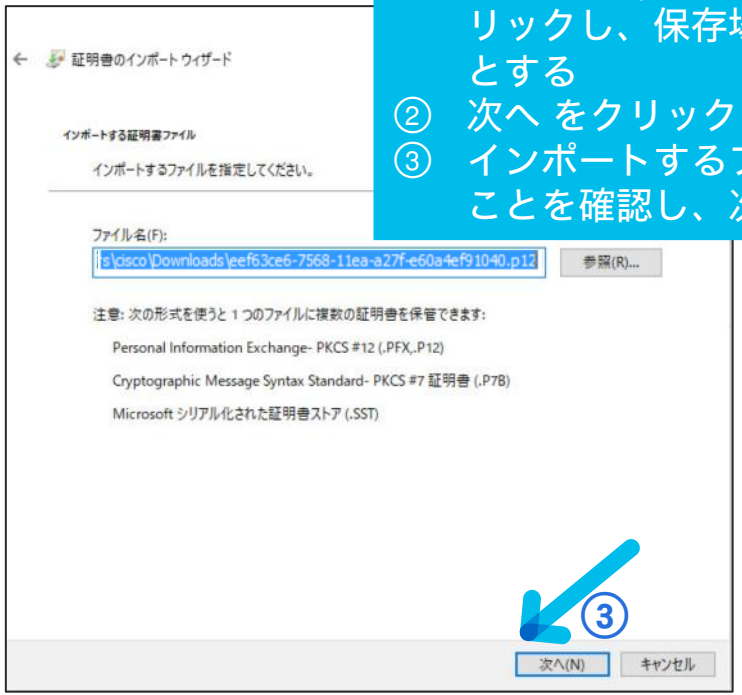
① 作成した Internal CA の Edit (鉛筆アイコン) をクリック
② Download をクリック
③ PKCS #12 ファイルの任意パスワードを設定した後、OKをクリック
④ PKCS #12 ファイルが自動ダウンロードされる

ステップ2-2: PC への Internal CA 証明書のインポート(参考)

入手した Internal CA の PKCS #12 形式のファイルを、テスト PC にコピーし、インポートする。ここでは Windows 10 でのインポート手順を参考として記載

① 入手した .p12 ファイルをダブルクリックし、保存場所を現在のユーザーとする
② 次へ をクリック
③ インポートするファイルが合っていることを確認し、次へ　をクリック

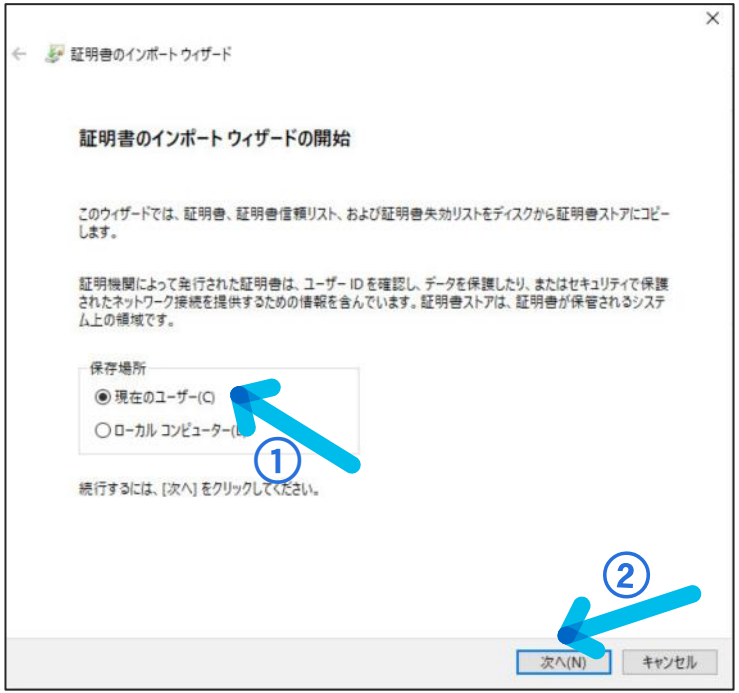


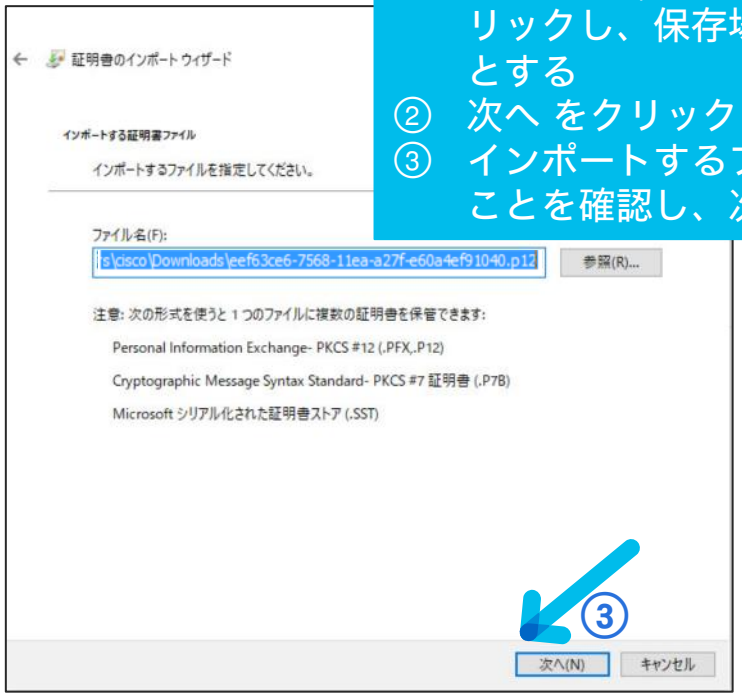


ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)

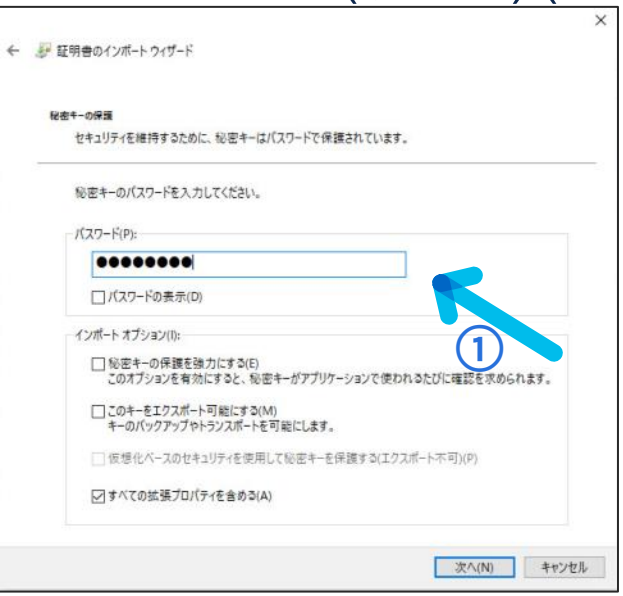
入手した Internal CA の PKCS #12 形式のファイルを、テスト PC にコピーし、インポートする。ここでは Windows 10 でのインポート手順を参考として記載

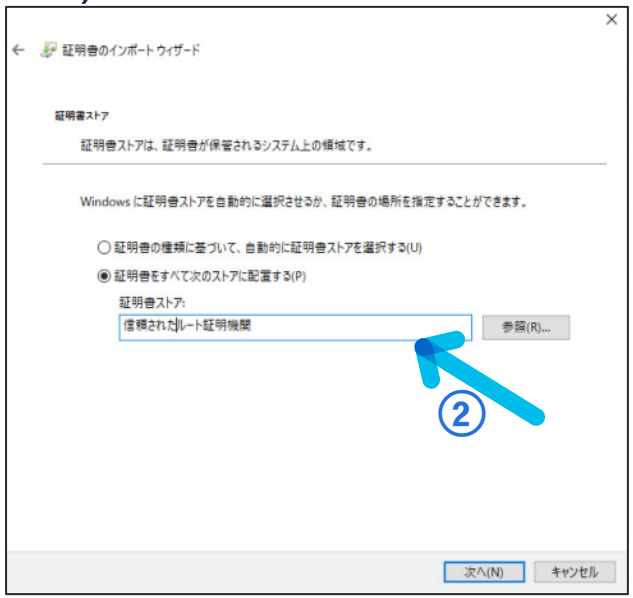
① 入手した .p12 ファイルをダブルクリックし、保存場所を現在のユーザーとする
② 次へ をクリック
③ インポートするファイルが合っていることを確認し、次へ　をクリック

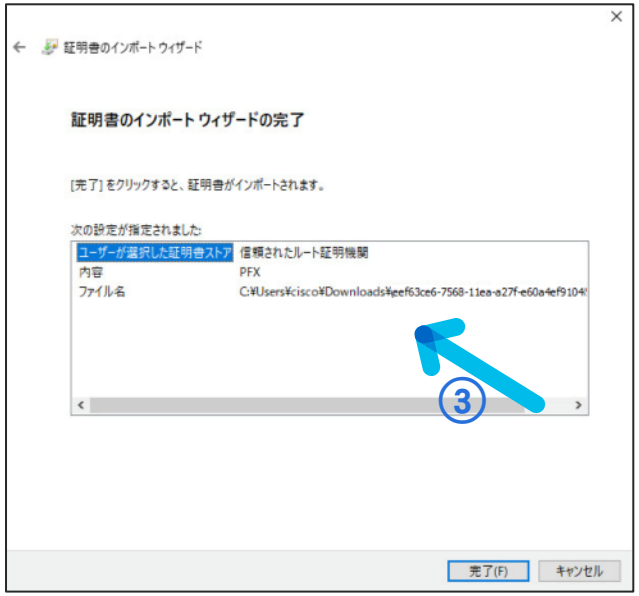




ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)

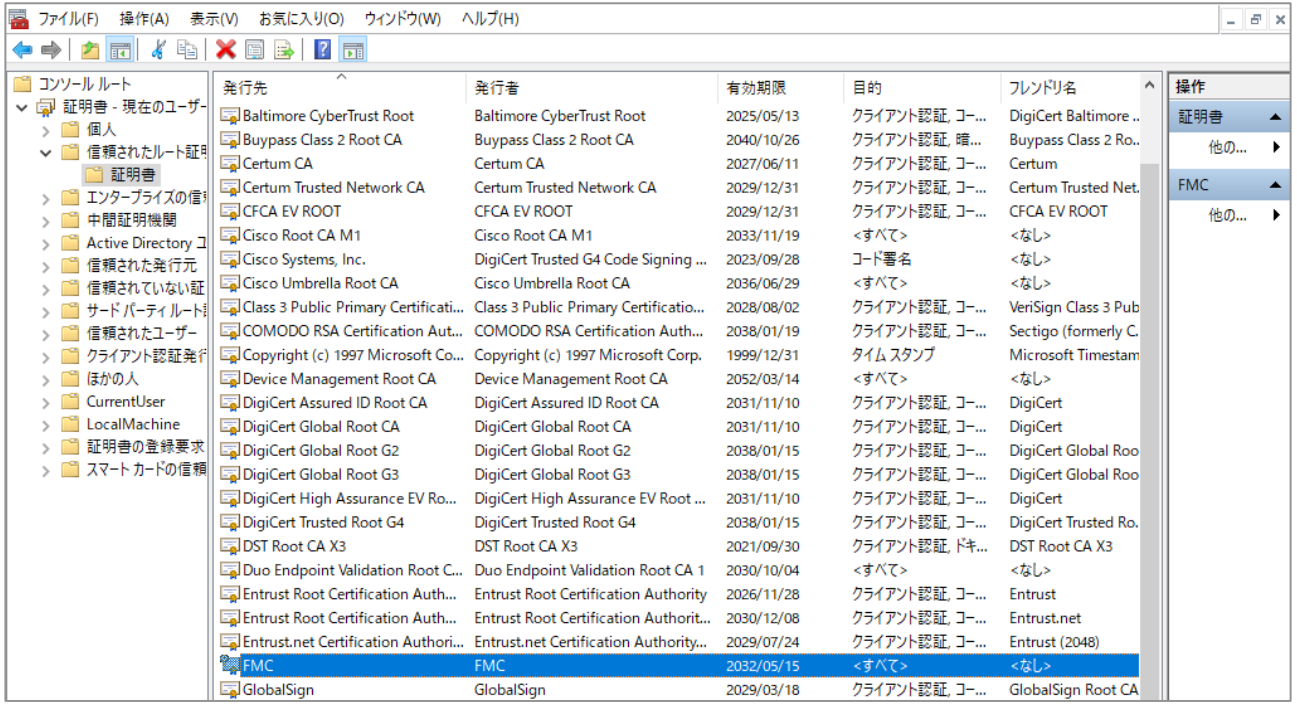






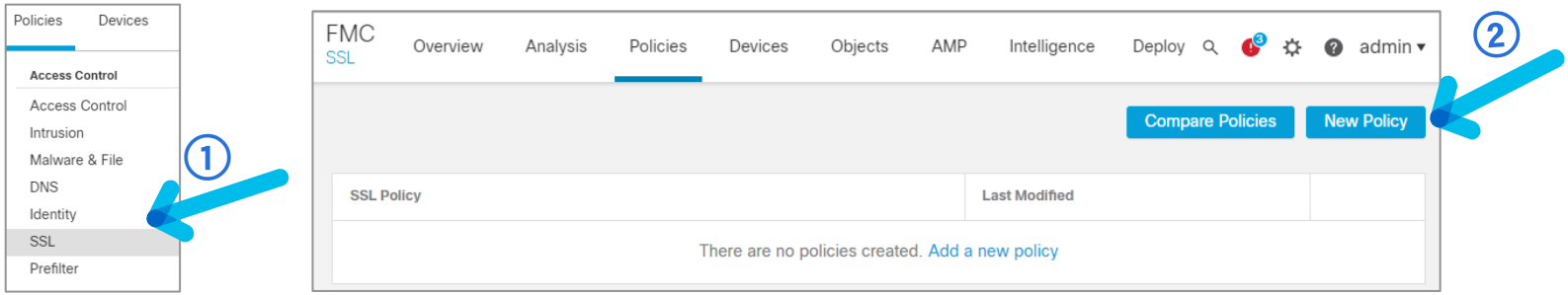
① FMC で設定した PKCS #12 のパスワードを入力し、次へ をクリック
② マニュアルで証明書ストアに「信頼されたルート証明機関」を選択し、次へ をクリック
③ ファイル名や証明書ストアが正しいことを確認し、次へ をクリック

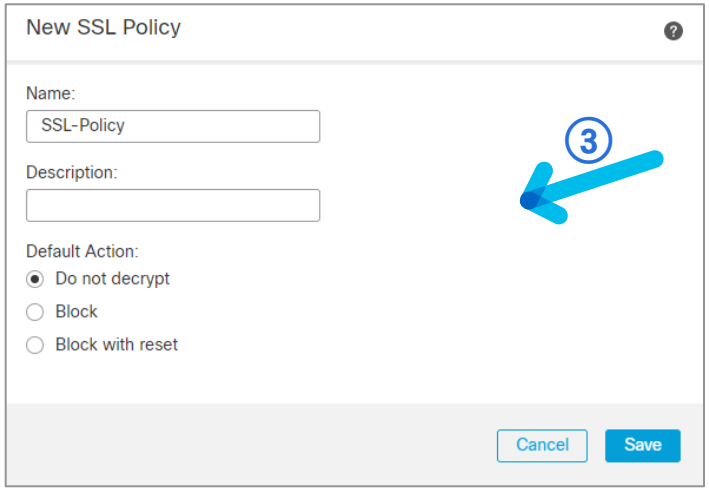
ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)



はい　をクリックすると Internal CA の証明書がインポートされる
Microsoft 管理コンソール (MMC) からインポートされた証明書が確認可能 (参考情報)

ステップ3-1: SSL policy の作成

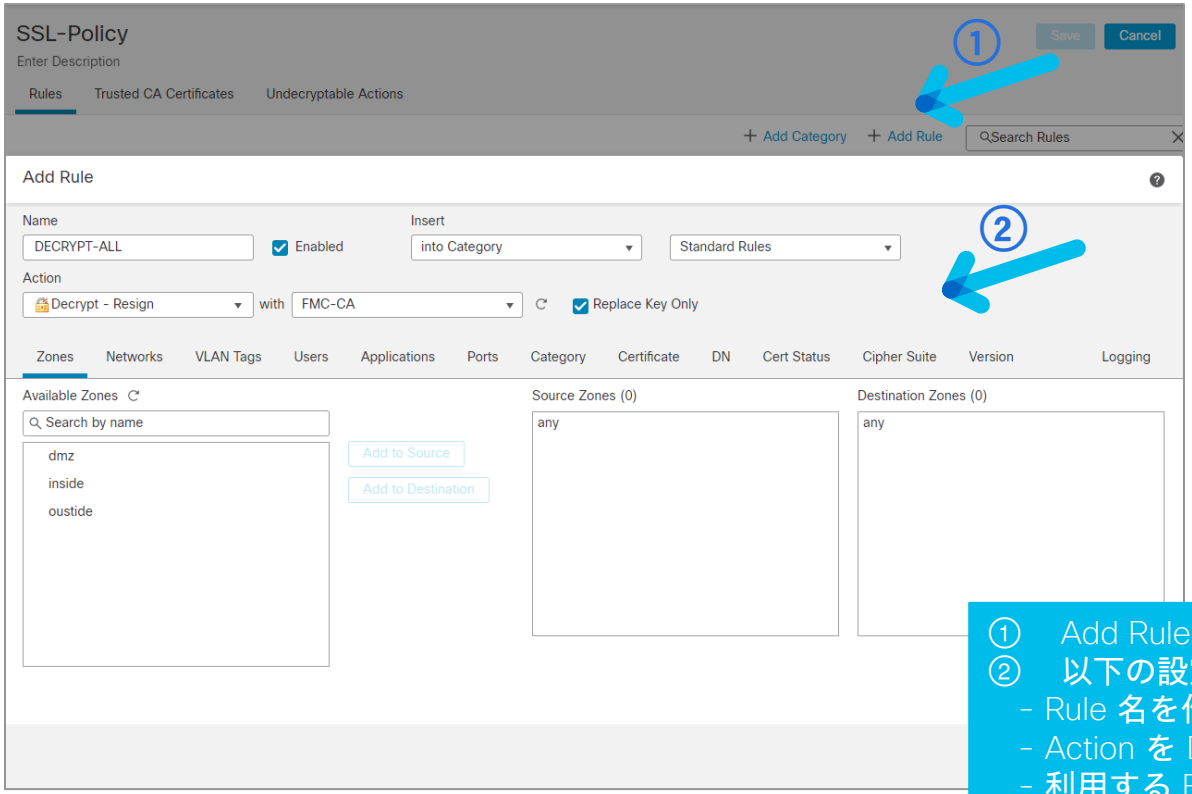




① FMC にて Policies > SSL を選択
② New Policy をクリック
③ 以下を入力し Save
- ポリシー名
- Default Action はそのまま (Do not decrypt) で

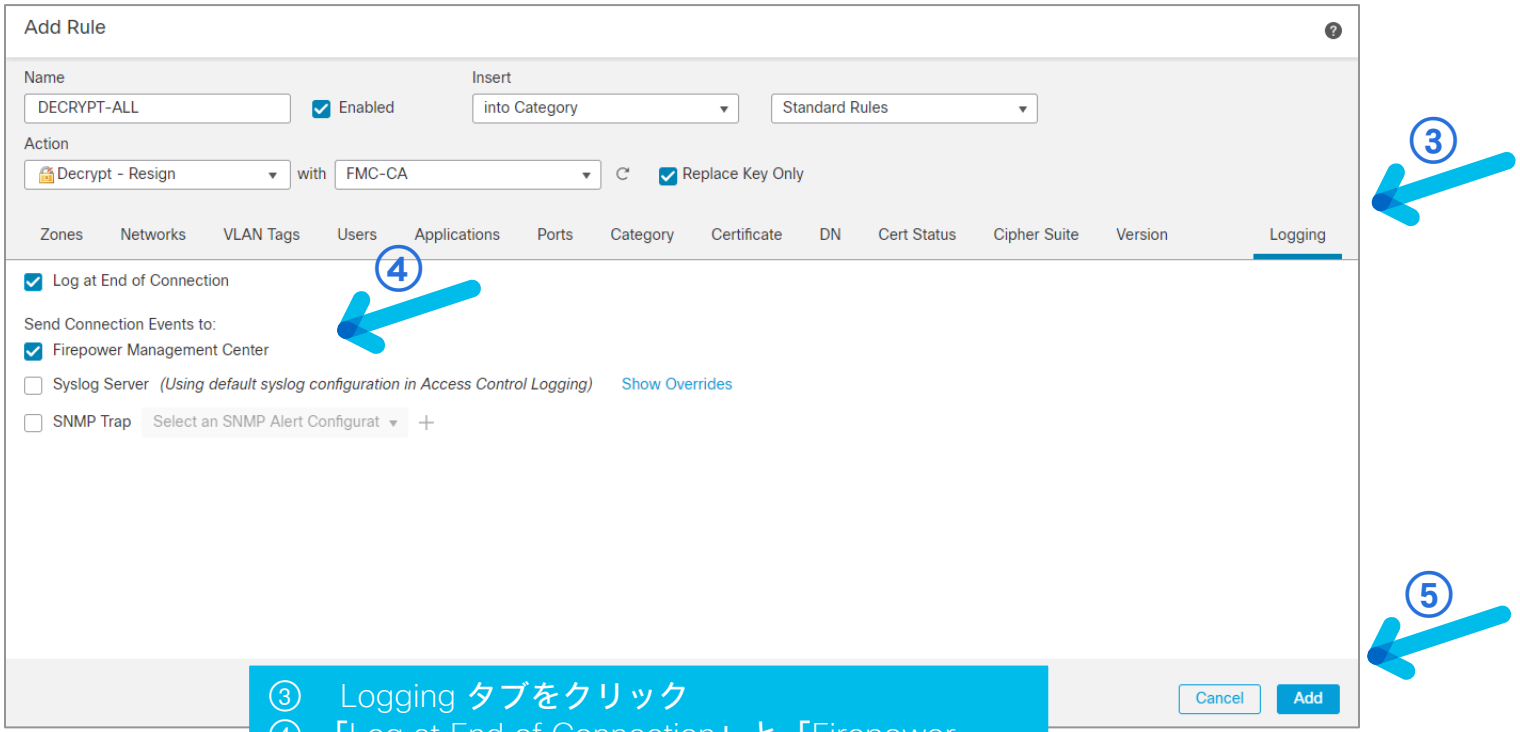
本シナリオでは、簡素化のため、すべての通信において TLS 復号を行うポリシーを適用する。 実際には、FTD の負荷軽減のためにも、複合する通信としないののメリハリ分けを

ステップ3-2: SSL policy のルール作成



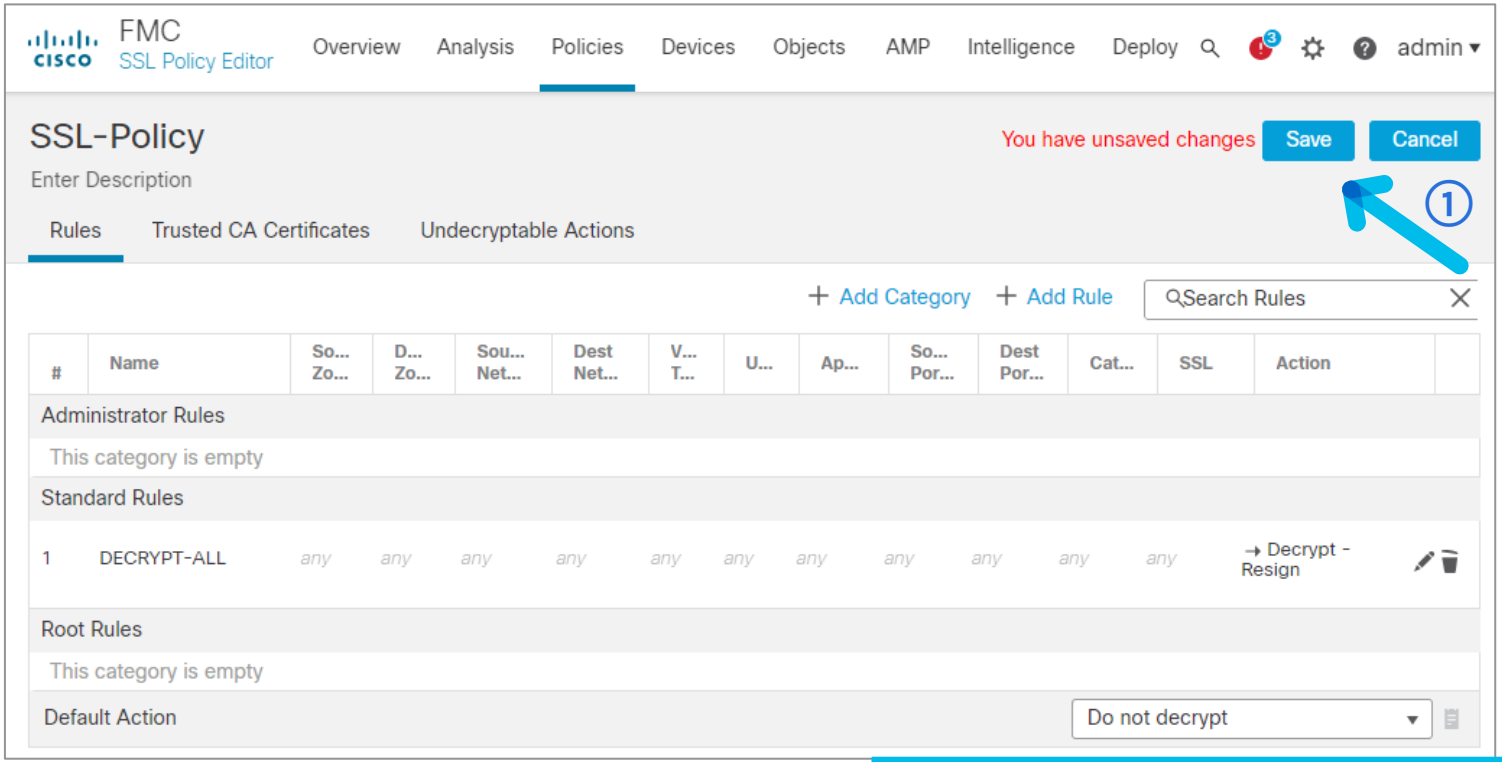
① Add Rule をクリック
② 以下の設定を行う
- Rule 名を作成し Enabled をクリック
- Action を Decrypt – Resign に
- 利用する FMC 証明書を選択

ステップ3-2: SSL policy のルール作成 (続き)



③ Logging タブをクリック
④ 「Log at End of Connection」と「Firepower Management Center」をチェック
⑤ Add ボタンをクリック

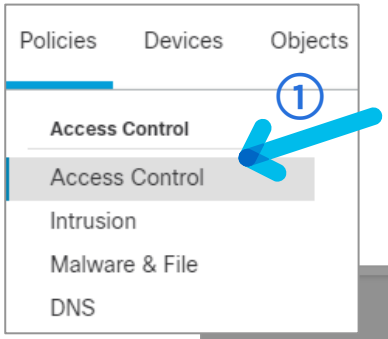
ステップ3-3: SSL policy のルール作成 (続き)

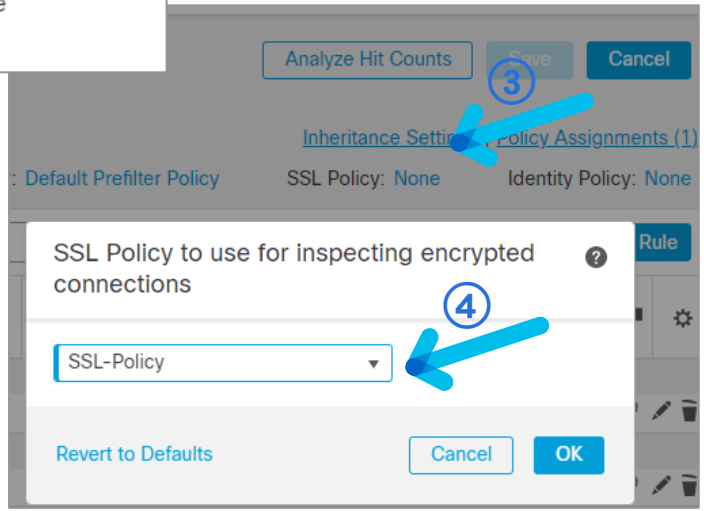


① 設定したルールに間違いがないことを確認した後、Save をクリック

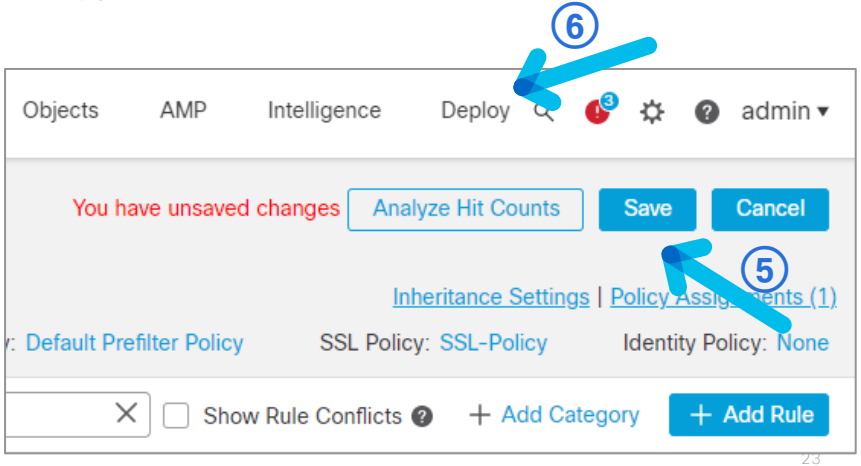
ステップ4: Access Control Policy と SSL Policy の紐付けとデプロイ

① Policies > Access Control を選択
② FTD で利用している ACP の鉛筆アイコン (edit) をクリック
③ SSL Policy をクリック
④ 作成した復号ポリシーを選択し OKをクリック
⑤ ACP 画面に戻って Save をクリック
⑥ Deploy をクリックし 対象デバイスに設定適用 (※)



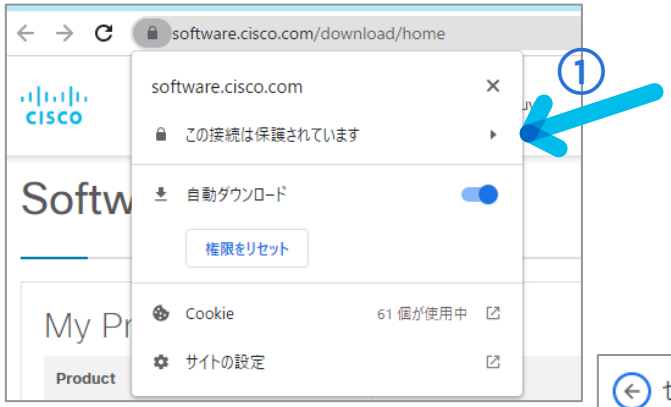


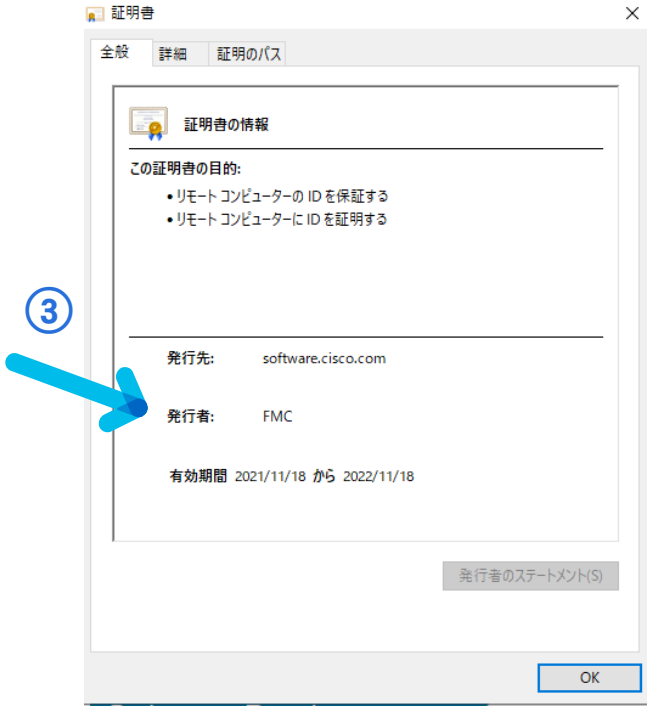
※SSLポリシーはデプロイ時 通信影響が発生するため
適用タイミングに注意



ステップ5-1: PC からの https サイトに疎通確認

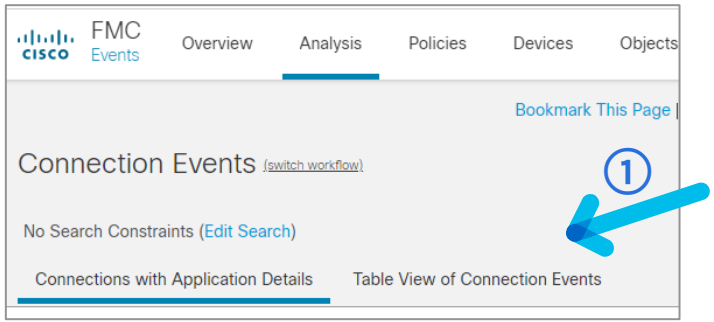
Deploy 終了後、動作確認を行う。テスト PC の Web ブラウザ (今回は Chrome を使用) から任意の https サイトにアクセスし、アドレスバーの鍵マークをクリックすることで、どの証明書を使い 暗号通信をしているか確認できる





テスト PC は FMC の Internal CA を
信頼しているため、https のエラーにならない

ステップ5-2: FMCでイベント確認



① FMC の Connection Events から、Table View を選択
② SSL Status という項目にて、その https の通信が復号 (outgoing の resign) されていることを確認できる

②

SSL Status ×	Application Protocol ×	Client ×	Client Version ×	Web Application ×	Application Risk ×	Business Relevance ×
Decrypt (Resign)	HTTPS	SSL client		Microsoft Windows Live Services Authentication	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		Microsoft	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		Microsoft Windows Live Services Authentication	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		Microsoft Windows Live Services Authentication	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		Microsoft Windows Live Services Authentication	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		Microsoft Windows Live Services Authentication	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		Microsoft Windows Live Services Authentication	Medium	Low
Decrypt (Resign)	HTTPS	SSL client		OneDrive	Medium	Medium

12. Identity(ID)FW の設定

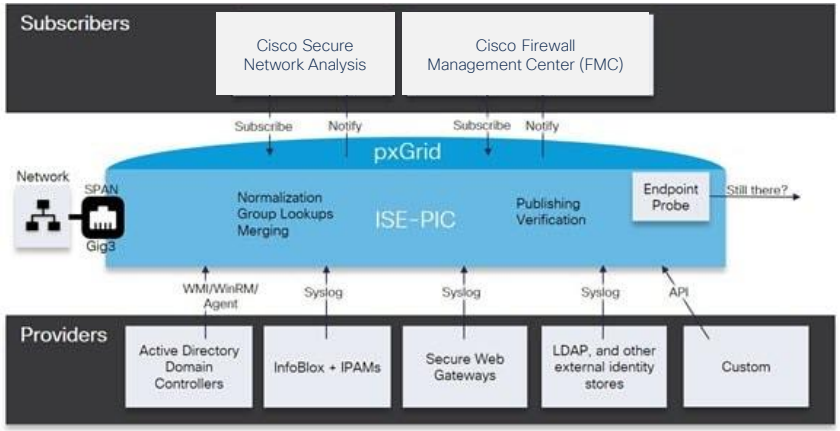
Identity Firewall 概要

- ユーザーアイデンティティ情報をトラフィックフローに関連付けることで可視性の強化、およびユーザ・グループベースでのトラフィック制御を実現
- 使用コンポーネント
  - Firepower Management Center (FMC)
  - Firepower Threat Defense (FTD)
  - Identity Source : ISE、または ISE Passive Identity Connector (ISE-PIC)
  - Identity Store : Active Directory、または LDAP
- FMC は Identity Source、および Identity Store からそれぞれ以下の情報を取得して、ユーザ情報の可視化およびポリシーに反映
  - Identity Source : ユーザと IP アドレスのマッピング情報を FMC に提供
  - Identity Store : FMC の Realm (レルム) で設定された AD または LDAP から取得されるユーザとグループ情報。ポリシー作成に利用。

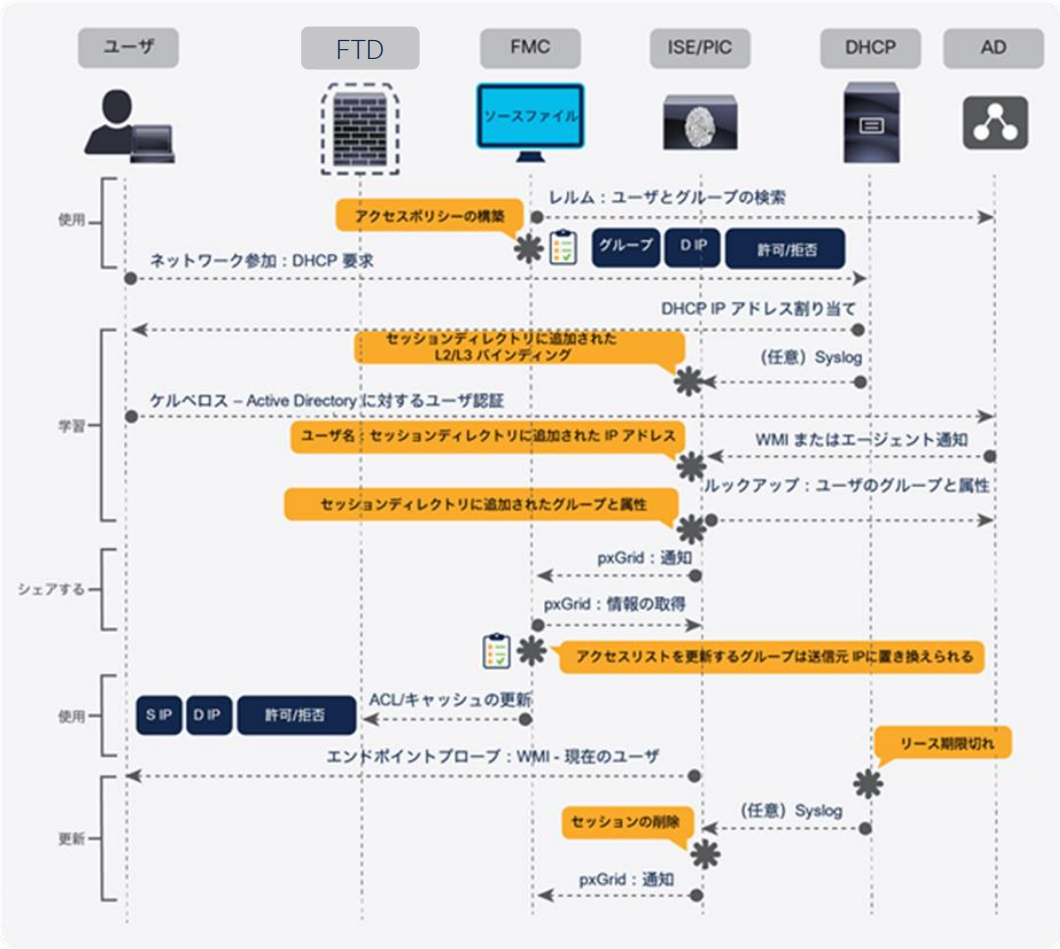
※注：Firepower 7.0 Identity Source として User Agent は利用できない

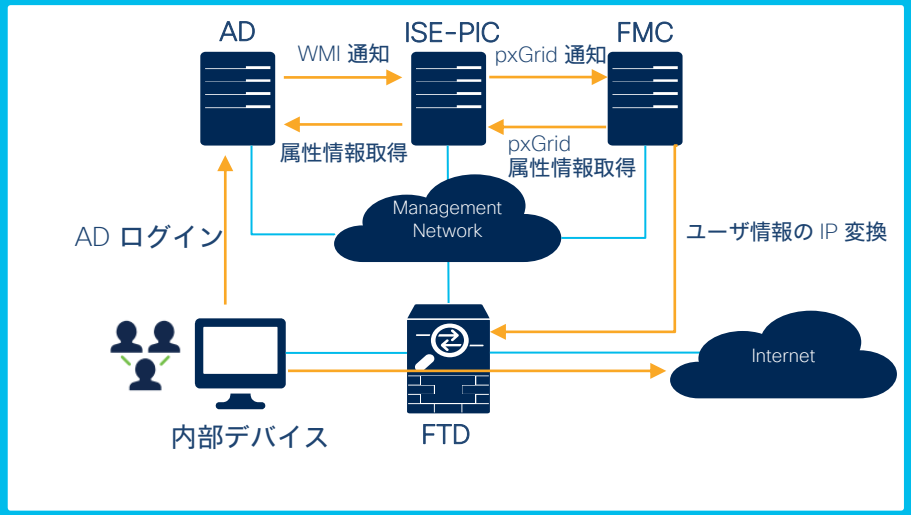
ISE / ISE Passive Identity Connector (ISE-PIC)

- FMC の Identity Source として動作
- パッシブ認証によって AD より取得したユーザおよび IP のマッピング情報を pxGrid を介して FMC に送信
- ISE-PIC は ISE の簡易版 (安価版) であり、パッシブ認証に特化した製品
- パッシブ認証とは
  - 直接の認証行為を行わず、プロバイダと呼ばれる Microsoft Active Directory (AD) などの信頼されたサードパーティシステムからネットワーク上のユーザのユーザ ID や IP アドレスなどの属性情報をパッシブに学習する技術
  - ISE / ISE-PIC は WMI や DC 上にインストールされた ISE-PIC エージェントなどを使用して AD からドメインユーザのログインと更新の通知を受け取る
    - WMI の利用を推奨



参考：FMC – ISE / ISE-PIC ワークフロー

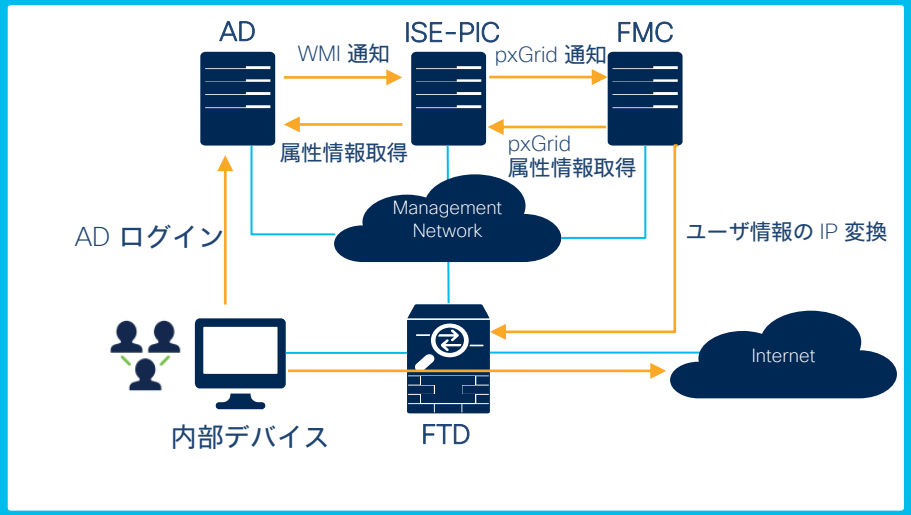




本ガイドでは Identity Source として ISE-PIC を使用

IDFW 設定ステップ
(FMC – ISE-PIC インテグレーション)

1. ISE-PIC のインストール、初期セットアップ
2. ISE-PIC での AD Join 設定
3. ISE-PIC での Root CA のダウンロードと FMC へのインポート
4. FMC での Internal CA の作成とダウンロード
5. OpenSSL による FMC Internal CA ファイルの形式変換 (PKCS#12 → PEM, Key)
6. FMC での Internal Cert のインポート
7. ISE-PIC での FMC Internal CA (PEM) のインポート
8. ISE-PIC での pxGrid の有効化
9. FMC での Identity Source の設定とテスト



本ガイドでは Identity Source として ISE-PIC を使用

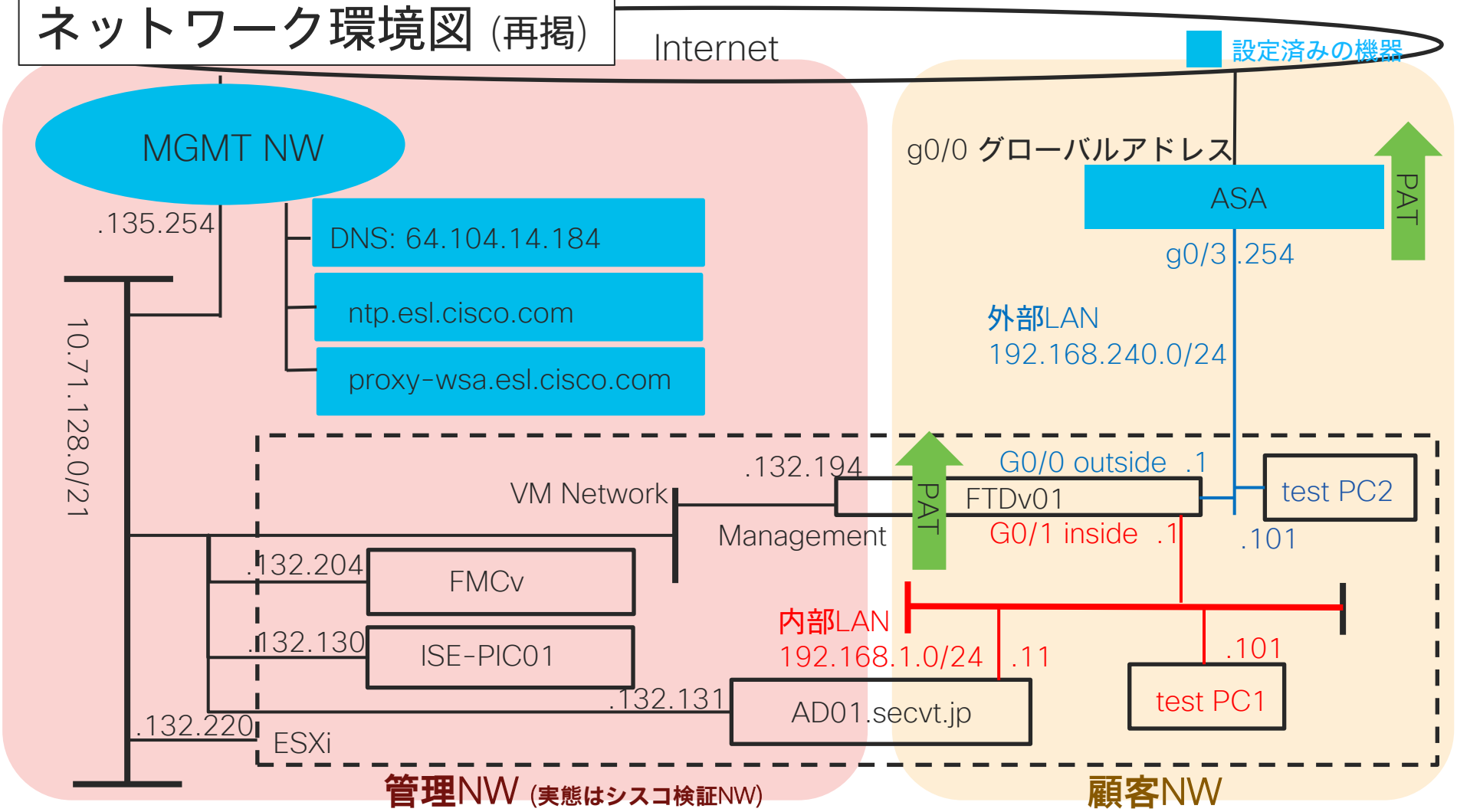
IDFW 設定ステップ
(FMC での Identity Policy 設定)

10. Realm の設定
11. Network Discovery での User の追加
12. Identity Policy の作成
13. ACP への Identity Policy の適用
14. 接続テスト

本セットアップガイドでの設定条件

- Identity Source として ISE-PIC v3.1 を利用
- Identity Store として AD (Windows Server 2016) を利用し (domain : secvt.jp)、Test PC1 をドメイン参加
- 必要コンポーネント (AD、ISE-PIC) はすでにインストール済でありこのガイドでは解説しない
  - ISE-PIC Installation Guide
    https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/pic_install_upgrade/b_pic_install_upgrade_31.html
- FMC – ISE-PIC 間の pxGrid 連携で使用される証明書はそれぞれ自己証明書を使用
  - 証明書内に記載されている FQDN ホストの名前解決が行えるようADで設定済
- 本構成では管理ネットワークとユーザーネットワークのルーティングが行えないため、ユーザーネットワーク (192.168.1.0/24) と AD の通信経路を別途確保 (次頁構成図参照)
  - IDFW を利用しない環境においては、管理ネットワークとユーザーネットワークが分離されている方が望ましいデザインであり、本環境は本来は IDFW を利用するようなデザインにはなっていないため、一時的な対応として AD をマルチホームで運用

ネットワーク環境図 (再掲)

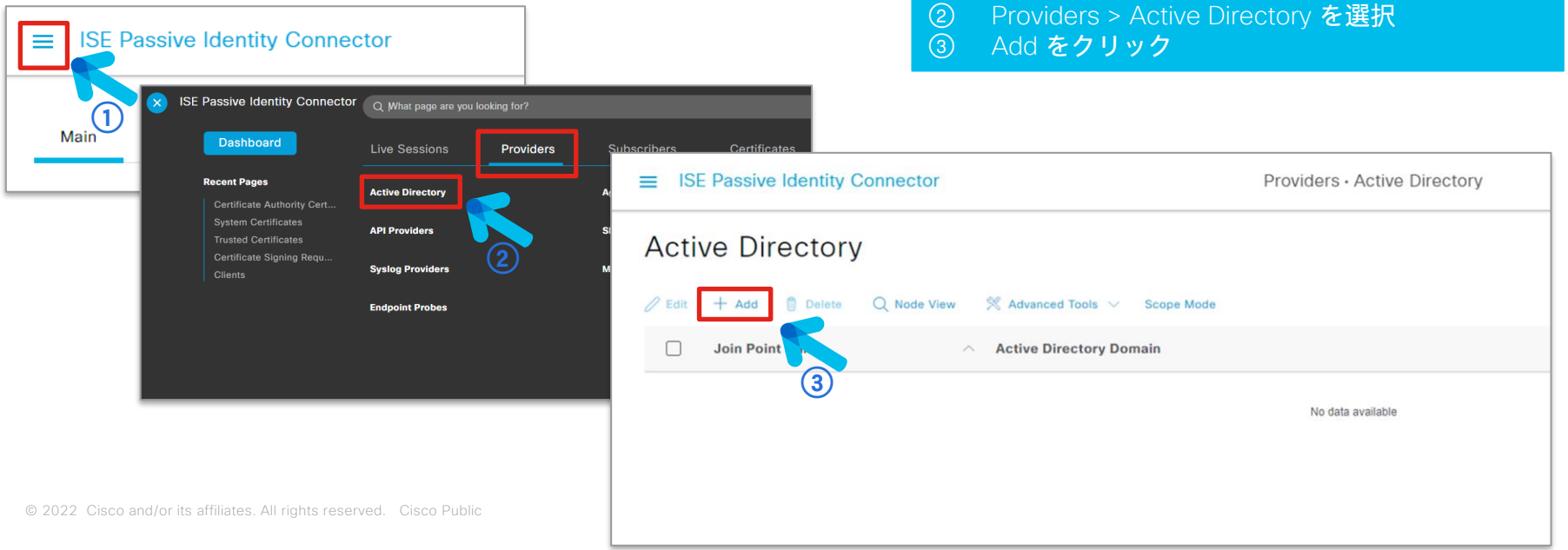


ISE-PIC での AD Join 設定

- ISE-PIC にてパッシブ ID サービスのプロバイダとなる AD を登録

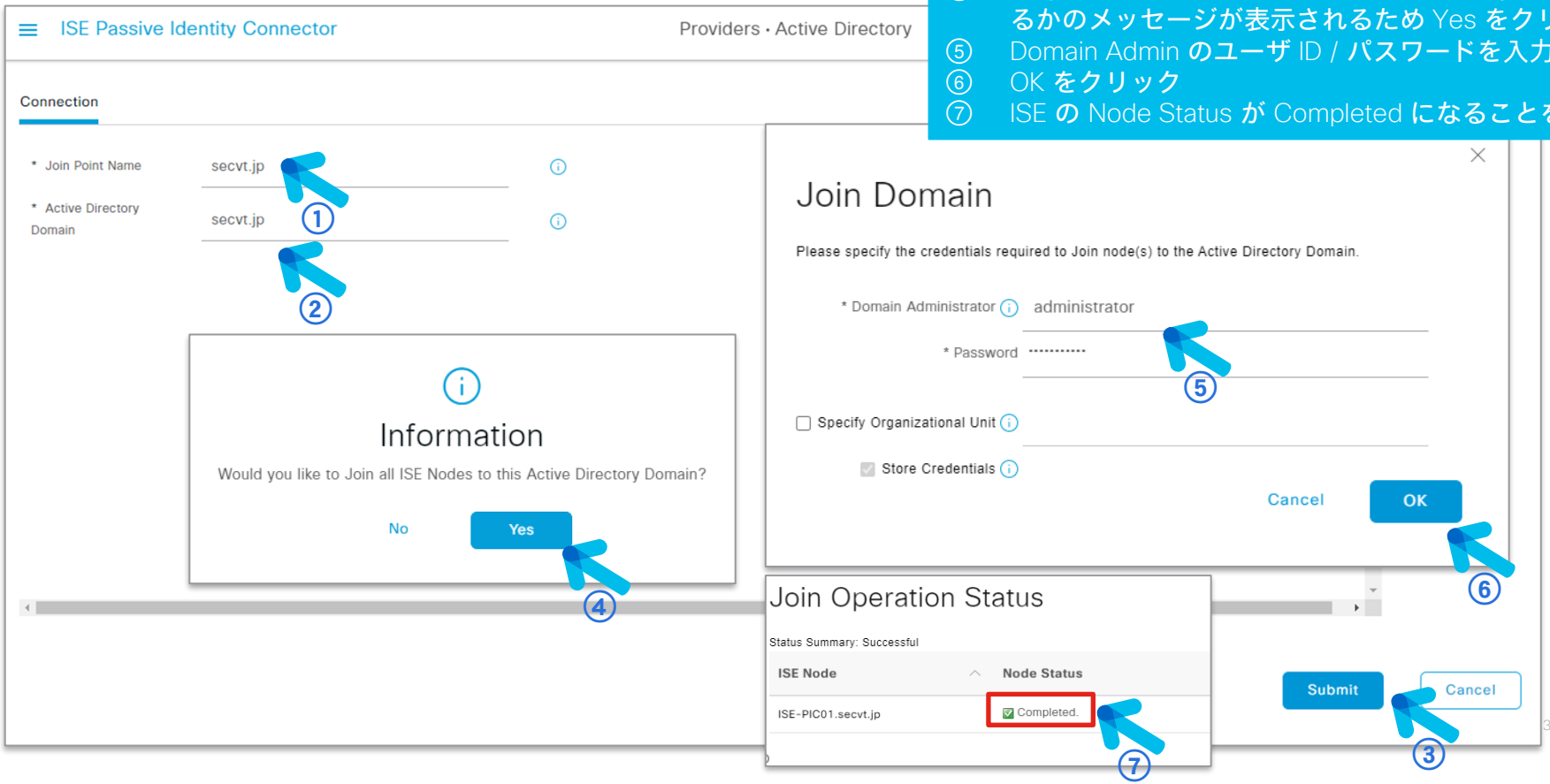
  Providers > Active Directory

① ISE-PIC にログイン後、左上のメニューアイコンをクリック
② Providers > Active Directory を選択
③ Add をクリック



ISE-PIC での AD Join 設定

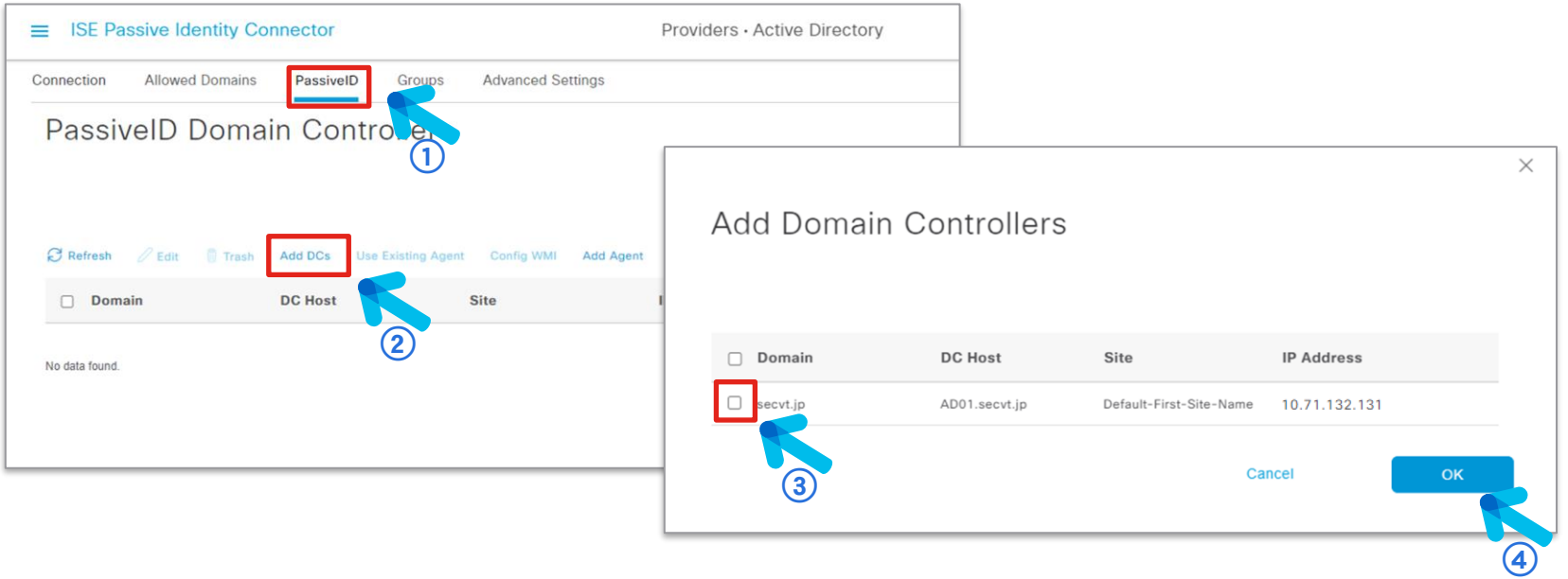
① 任意の名前を入力
② AD のドメインを入力
③ 右下の Submit をクリック
④ 登録したドメインにすべての ISE ノードを参加させるかのメッセージが表示されるため Yes をクリック
⑤ Domain Admin のユーザ ID / パスワードを入力
⑥ OK をクリック
⑦ ISE の Node Status が Completed になることを確認



ISE-PIC での AD Join 設定

- 追加でパッシブ ID サービス設定を実施

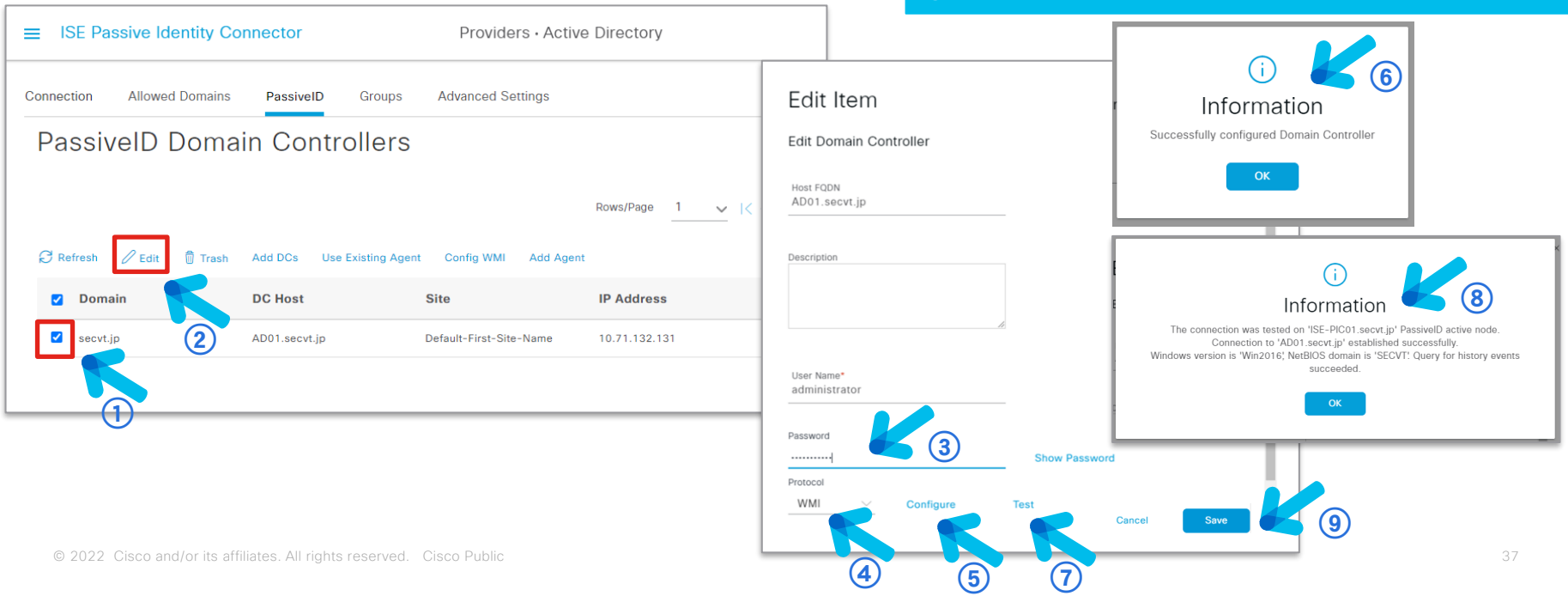
① PassiveID を選択
② Add DCs を選択
③ 先ほど登録した secvt.jp ドメインが表示されるのでチェックを入れる
④ OK をクリック



ISE-PIC での AD Join 設定

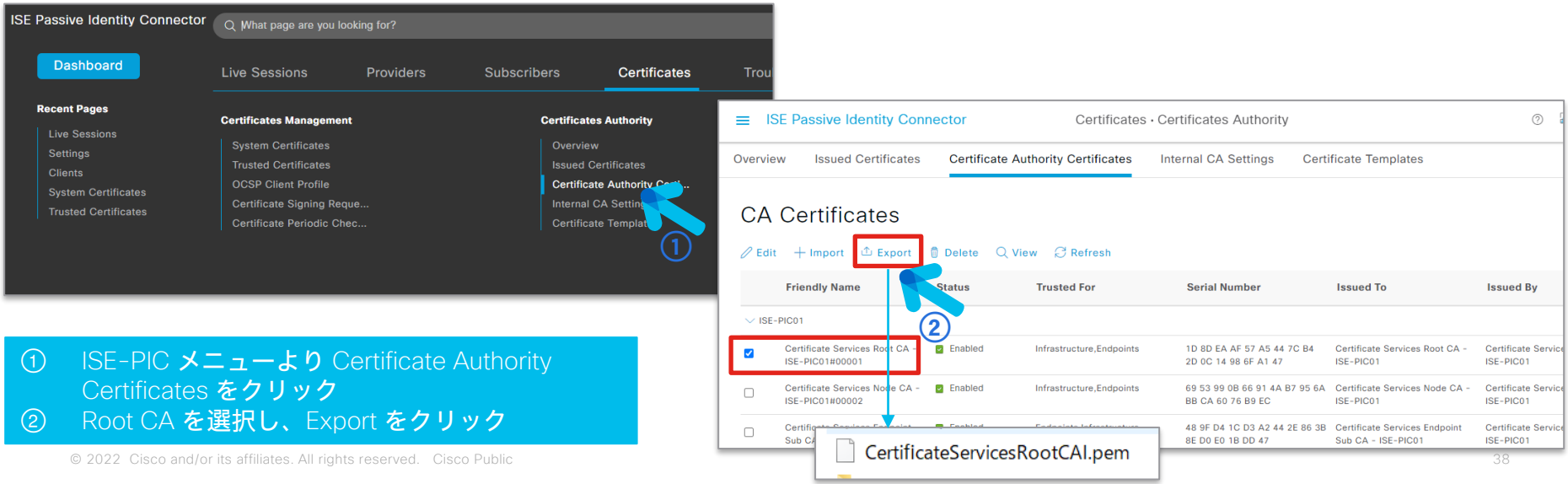
- 追加でパッシブ ID サービス設定を実施

① PassiveID DC に登録された secvt.jp を選択
② Edit を選択
③ AD admin の Password を入力
④ Protocol で WMI を選択して Configure をクリック
⑤ Information Successfully の Pop-up が出れば OK
⑥ Test をクリック
⑦ Information で Successfully の Pop-up が出れば OK
⑧ Save をクリック



ISE-PIC での Root CA のダウンロードと FMC へのインポート

- ISE-PIC – FMC 間は証明書を用いてセキュアな接続を行う。今回自己証明書を使用するため、はじめに ISE-PIC の Root CA (自己証明書) をダウンロードして FMC にインポートする
  Certificates > Certificates Authority > Certificates Authority Certificates

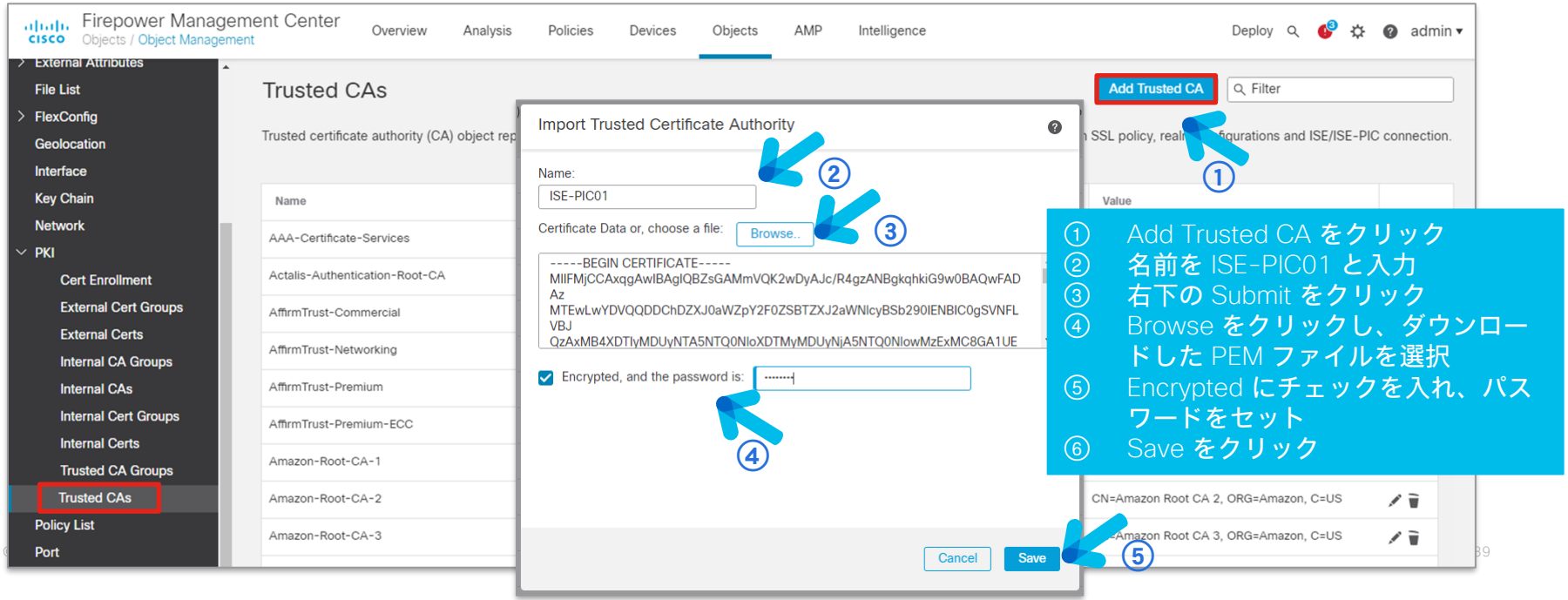


① ISE-PIC メニューより Certificate Authority Certificates をクリック
② Root CA を選択し、Export をクリック

ISE-PIC での Root CA のダウンロードと FMC へのインポー

- FMC の管理コンソールに移動し、ISE-PIC からダウンロードした Root CA を FMC にインポートする

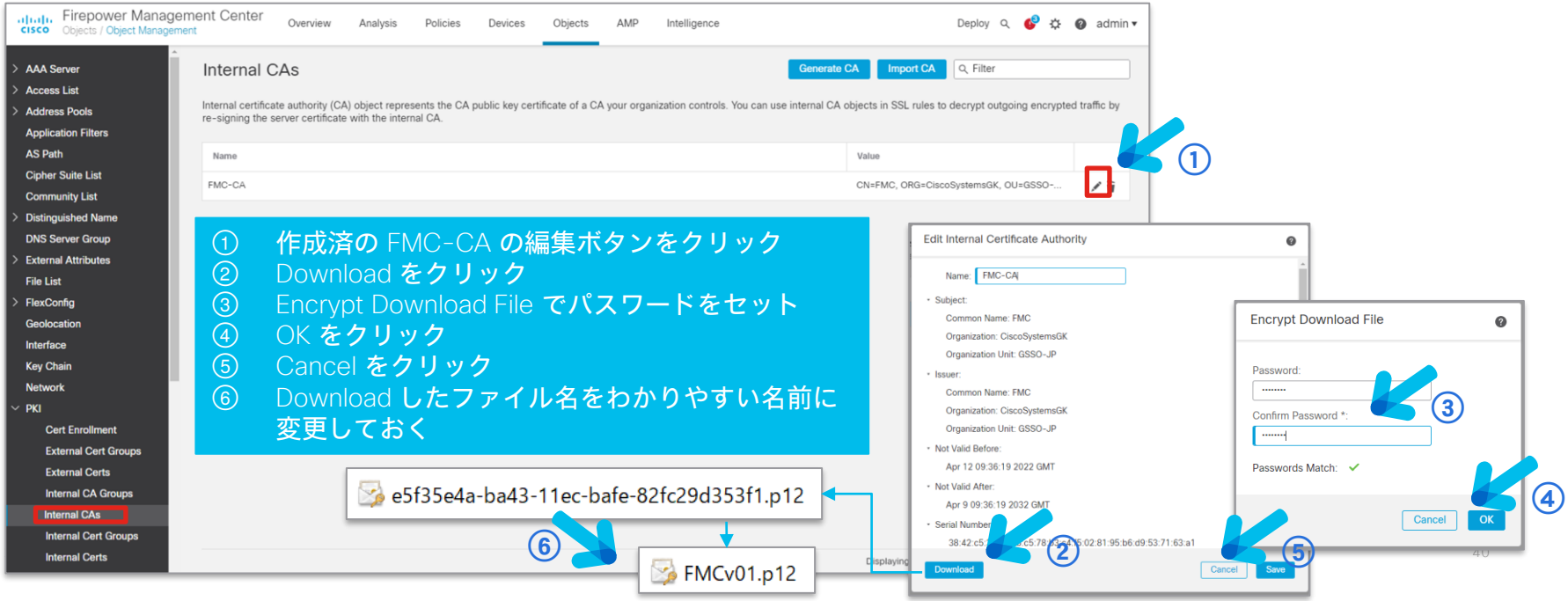
Objects > Object Management > PKI > Trusted CAs



FMC での Internal CA の作成およびダウンロード

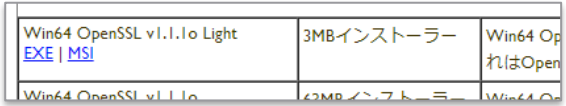
- FMC Internal CA は 11章 “TLS Decryption の設定” で作成済のためそれを活用する

Objects > Object Management > PKI > Internal CAs

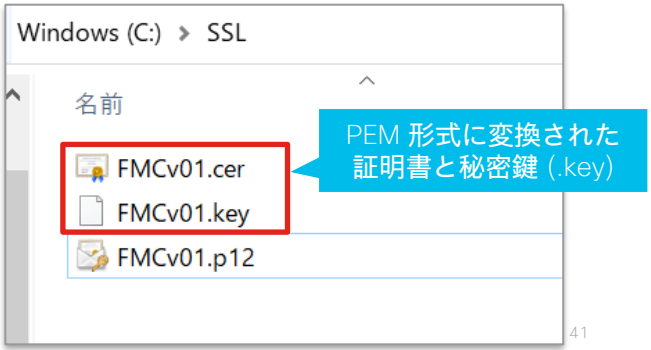


OpenSSL による FMC Internal CA ファイルの形式変換 (PKCS#12 → PEM, Key)

- FMC Internal CA の ISE-PIC へのインストールのためにファイル形式の変換 (PKCS#12 → PEM) が必要。また、ISE-PIC との接続に FMC は Internal Cert の証明書を使用し、作成済 Internal CA 証明書を Internal Cert にもインポートする必要があるが、こちらもインポートに PEM ファイルと秘密鍵がそれぞれ必要になるため、OpenSSL ソフトを利用して PKCS#12 ファイルからファイル形式を変換する
- 以下のサイトより Windows 10 版の OpenSSL をダウンロードし、端末にインストール
  - https://slproweb.com/products/Win32OpenSSL.html
  - 本ガイドでは Win64 OpenSSL v1.1.1o Light を利用
  - FMCv01.p12 が存在するディレクトリ上で以下のコマンドを実行



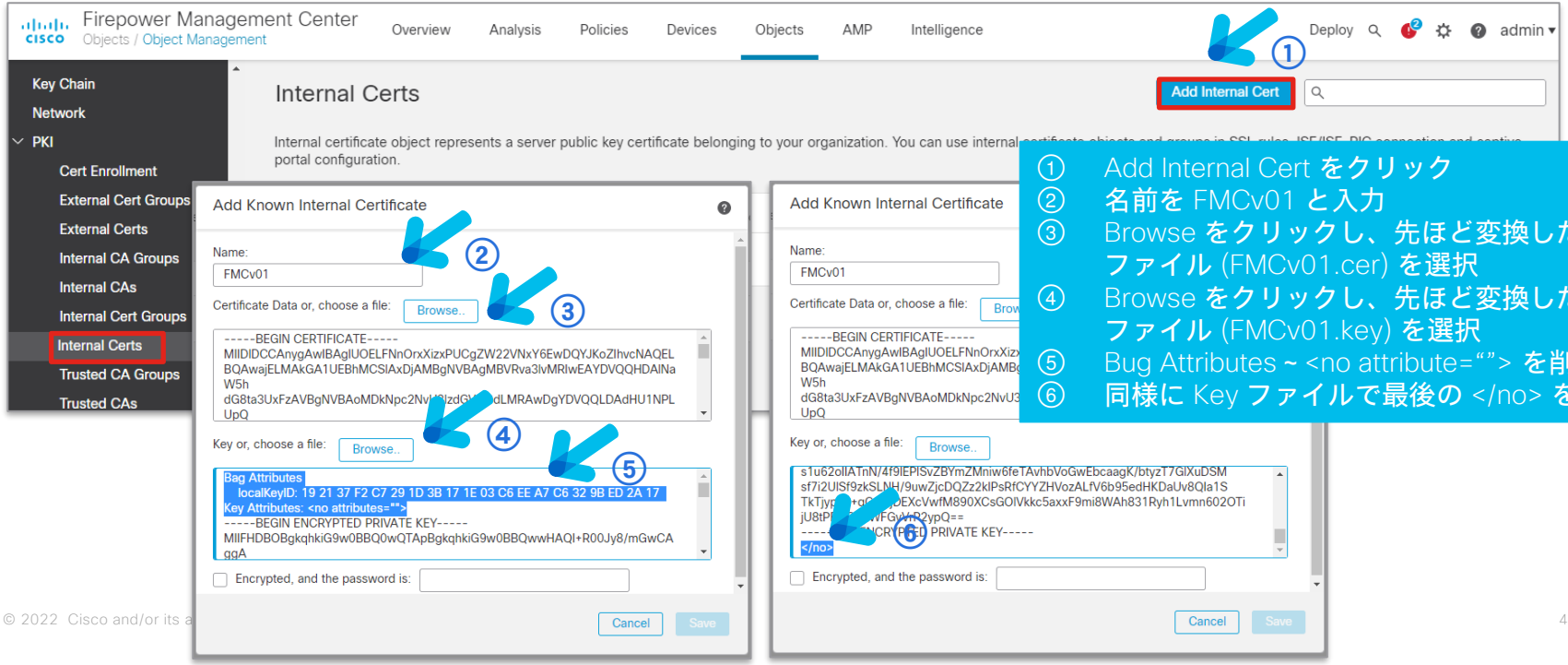

```
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:¥Users¥sinazawa>cd C:¥ssl

C:¥SSL>openssl pkcs12 -nokeys -clcerts -in FMCv01.p12 -out FMCv01.cer
Enter Import Password:

C:¥SSL>openssl pkcs12 -nocerts -in FMCv01.p12 -out FMCv01.key
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

C:¥SSL>
```



FMC での Internal Cert のインポート

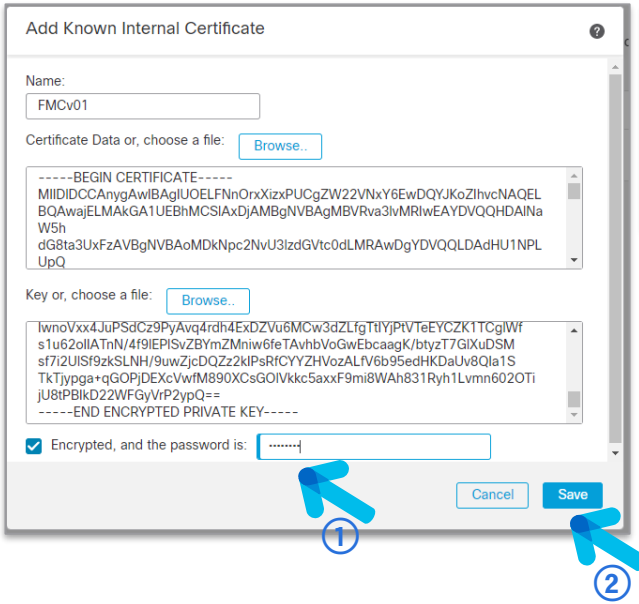
- 変換したファイルを使い、FMC の Internal Cert に証明書をインポートする

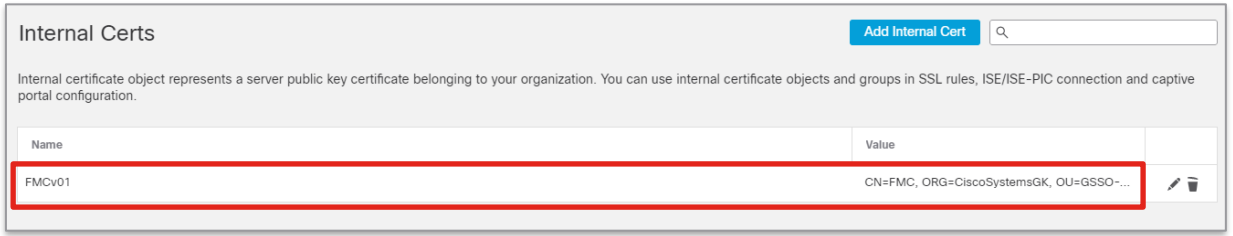
Objects > Object Management > PKI > Internal Certs



① Add Internal Cert をクリック
② 名前を FMCv01 と入力
③ Browse をクリックし、先ほど変換したPEM ファイル (FMCv01.cer) を選択
④ Browse をクリックし、先ほど変換した Key ファイル (FMCv01.key) を選択
⑤ Bug Attributes ~ <no attribute=“”> を削除
⑥ 同様に Key ファイルで最後の </no> を削除

FMC での Internal Cert のインポート



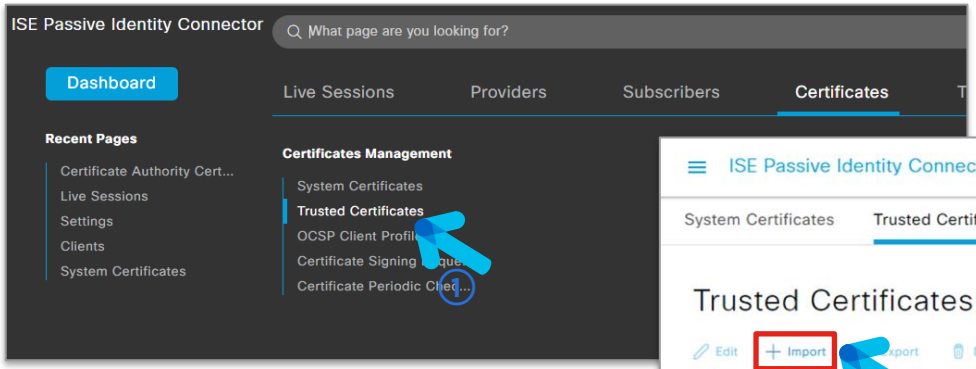


① Encrypted にチェックを入れてパスワードをセット
② Save をクリック

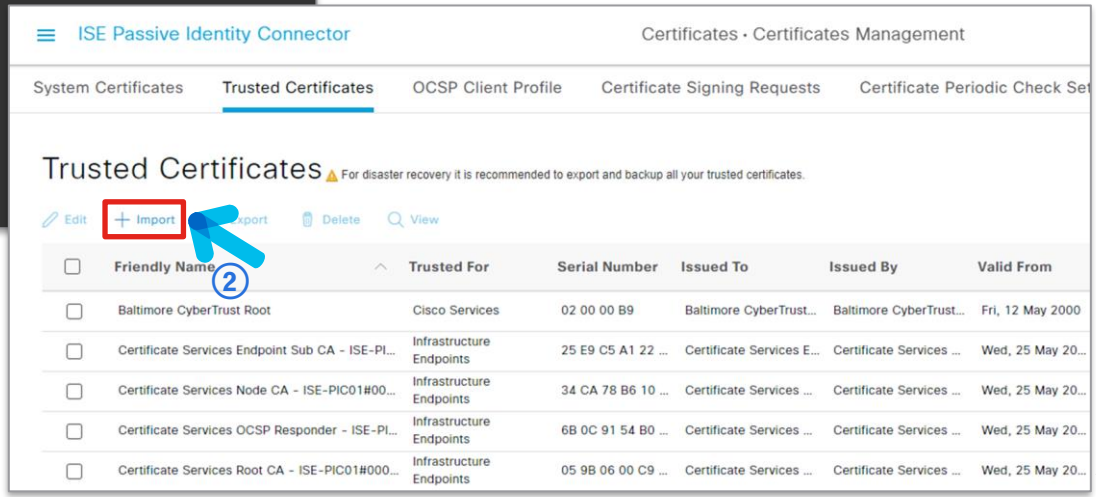
ISE-PIC での FMC Internal CA のインポート

- ISE-PIC にて FMC の Internal CA (変換した PEM ファイル) をインポート

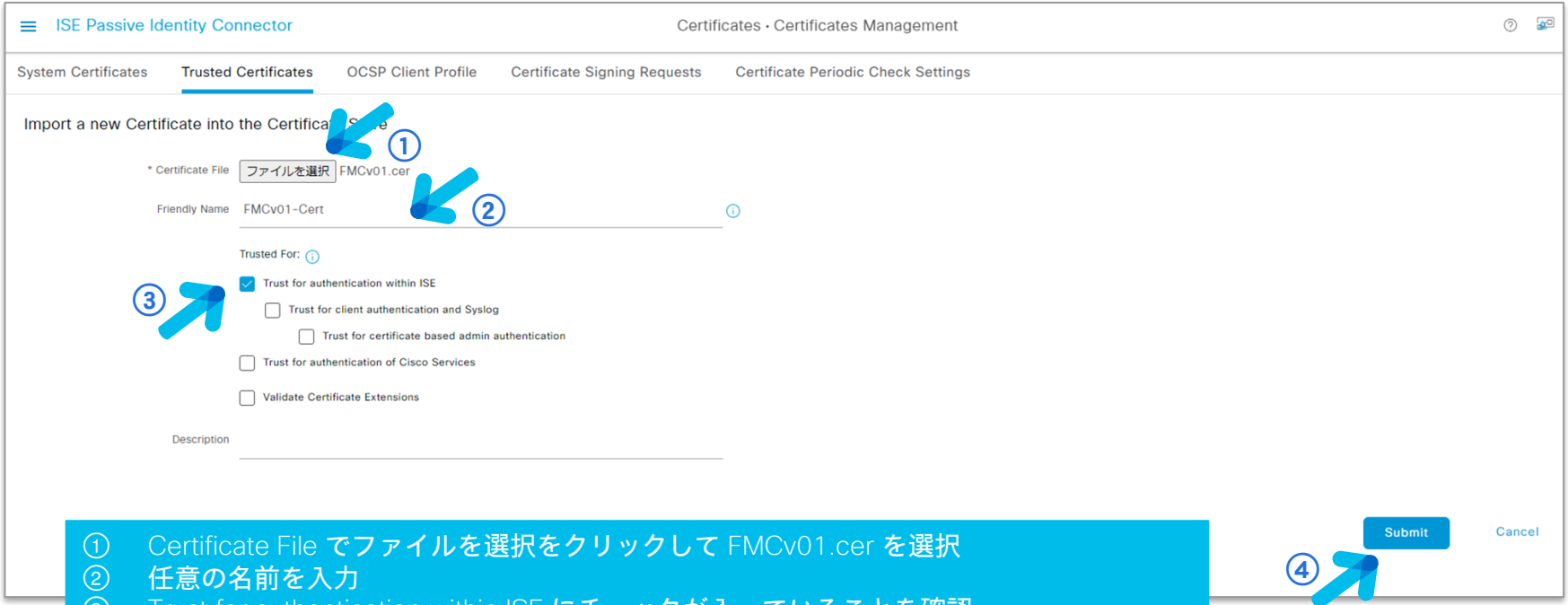
  Certificates > Certificates Management > Trusted Certificates



① ISE-PIC のメニューより Certificates > Certificates Management > Trusted Certificates を選択
② Import をクリック



ISE-PIC での FMC Internal CA のインポート



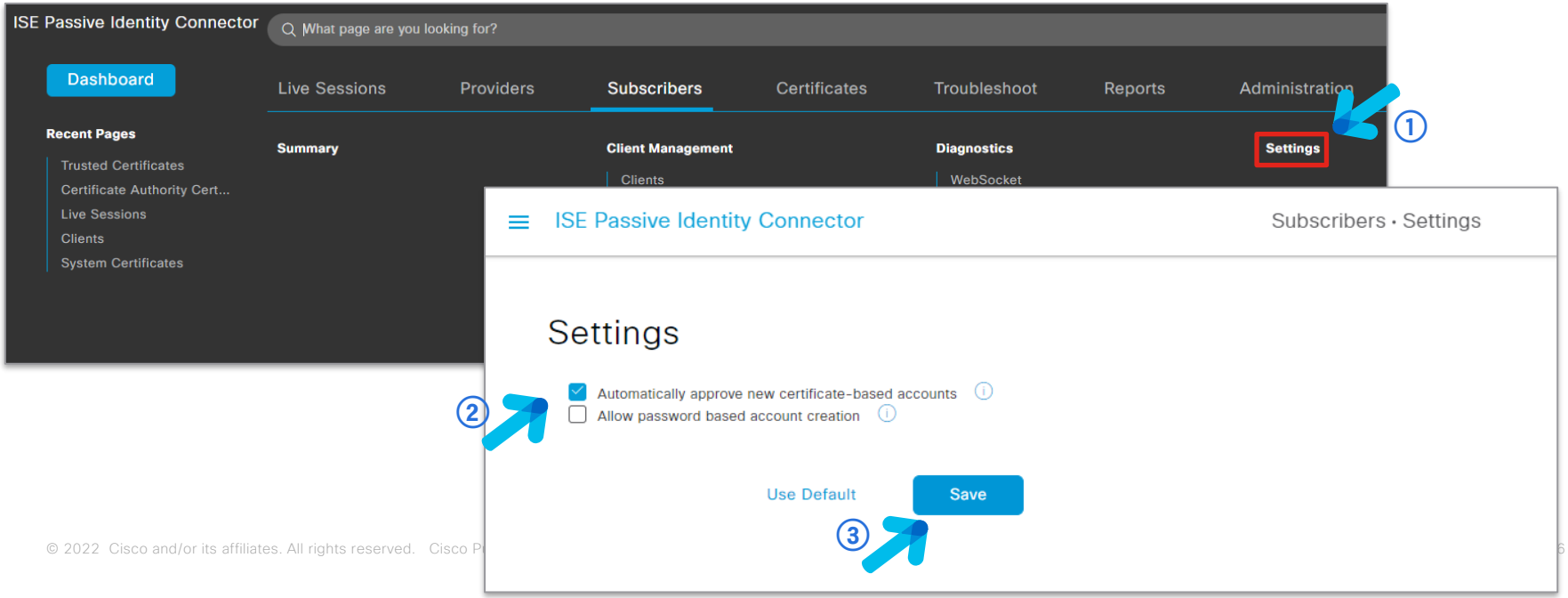
① Certificate File でファイルを選択をクリックして FMCv01.cer を選択
② 任意の名前を入力
③ Trust for authentication within ISE にチェックが入っていることを確認
④ Submit をクリック

ISE-PIC での pxGrid の有効化

- ISE-PIC にて pxGrid 連携でサブスクライバとなる FMC からの接続を許可するための設定を行う

Subscribers > Settings

① ISE-PIC のメニューより Subscribers > Settings を選択
② Automatically approve new certificate-base accounts にチェック
③ Save をクリック

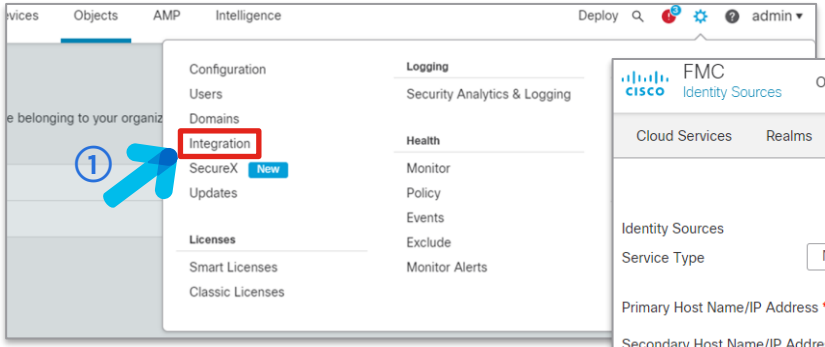


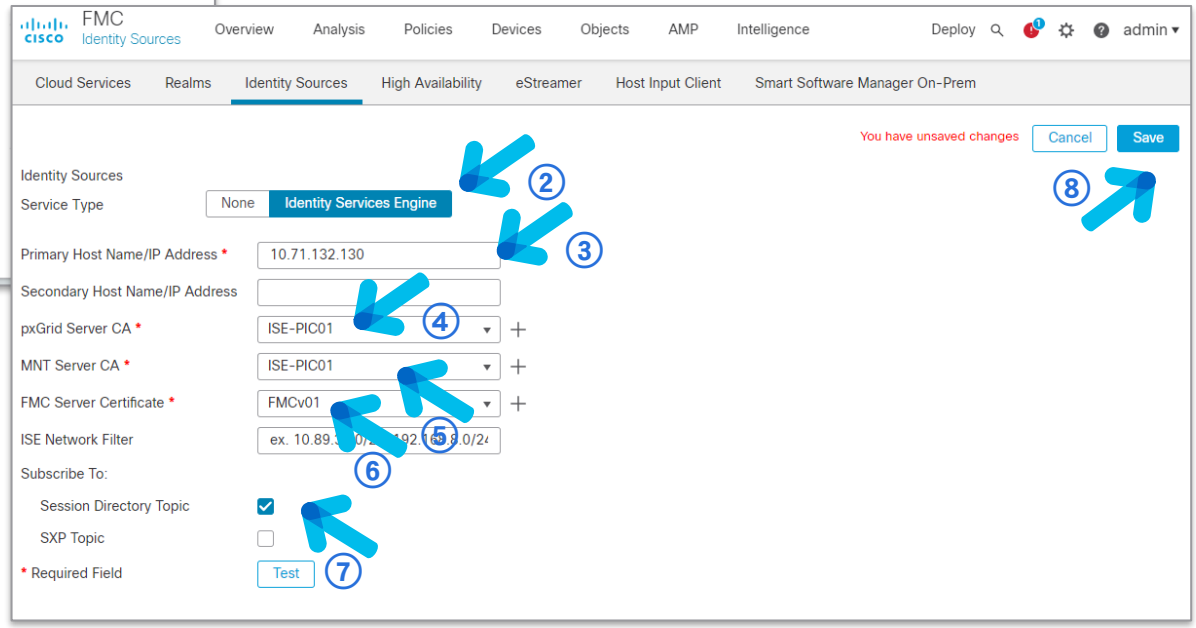
FMC での Identity Source の設定

- 最後に FMC の Identity Source の設定を実施

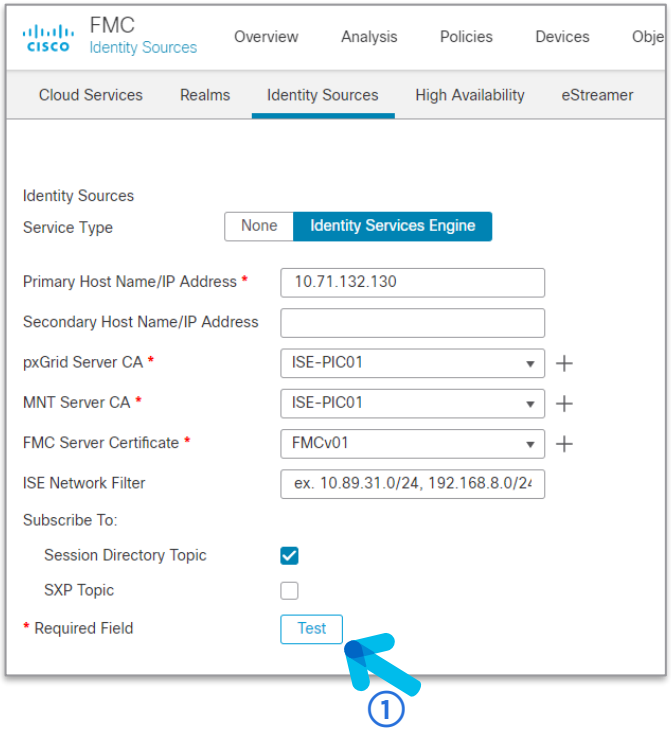
System > Integration > Identity Source

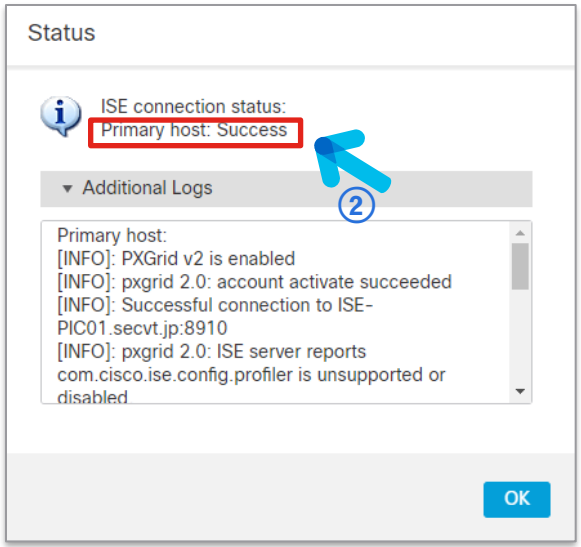
① Integration を選択
② Service Type でIdentity Services Engine を選択
③ ISE-PIC の IP アドレスを入力
④ pxGrid Server CA で ISE-PIC01 を選択
⑤ MNT Server CA で ISE-PIC01 を選択
⑥ FMC Server Certificate で FMCv01 を選択
⑦ Subscribe To で Session Directory Topic にチェックが入っていることを確認
⑧ Save をクリック





FMC – ISE-PIC 連携テスト



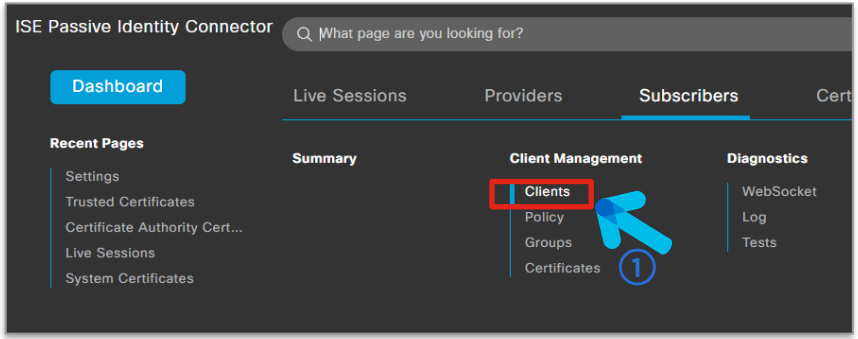


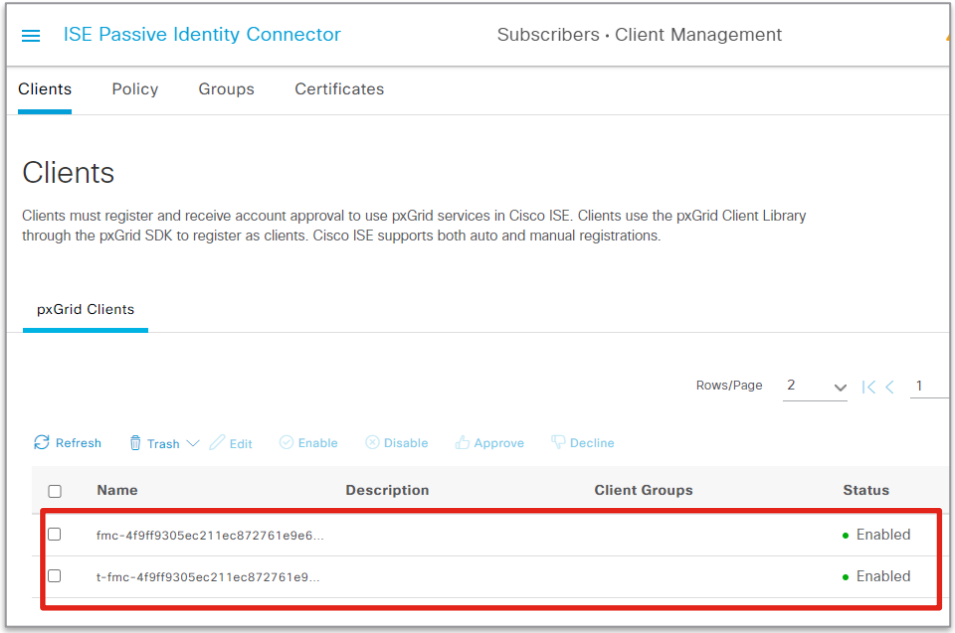
① Test をクリック
② Primary host: Success と表示されればテスト成功

FMC – ISE-PIC 連携テスト

- ISE-PIC での接続確認

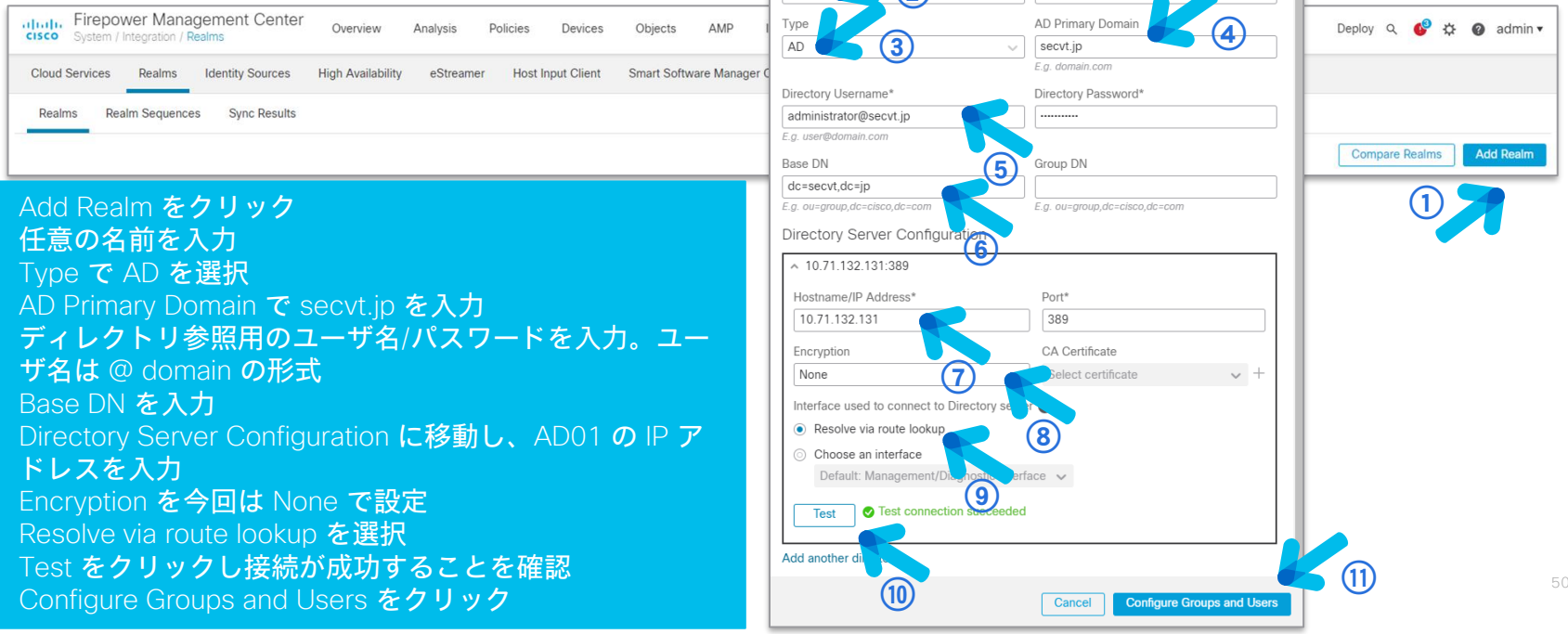
  Subscribers > Clients





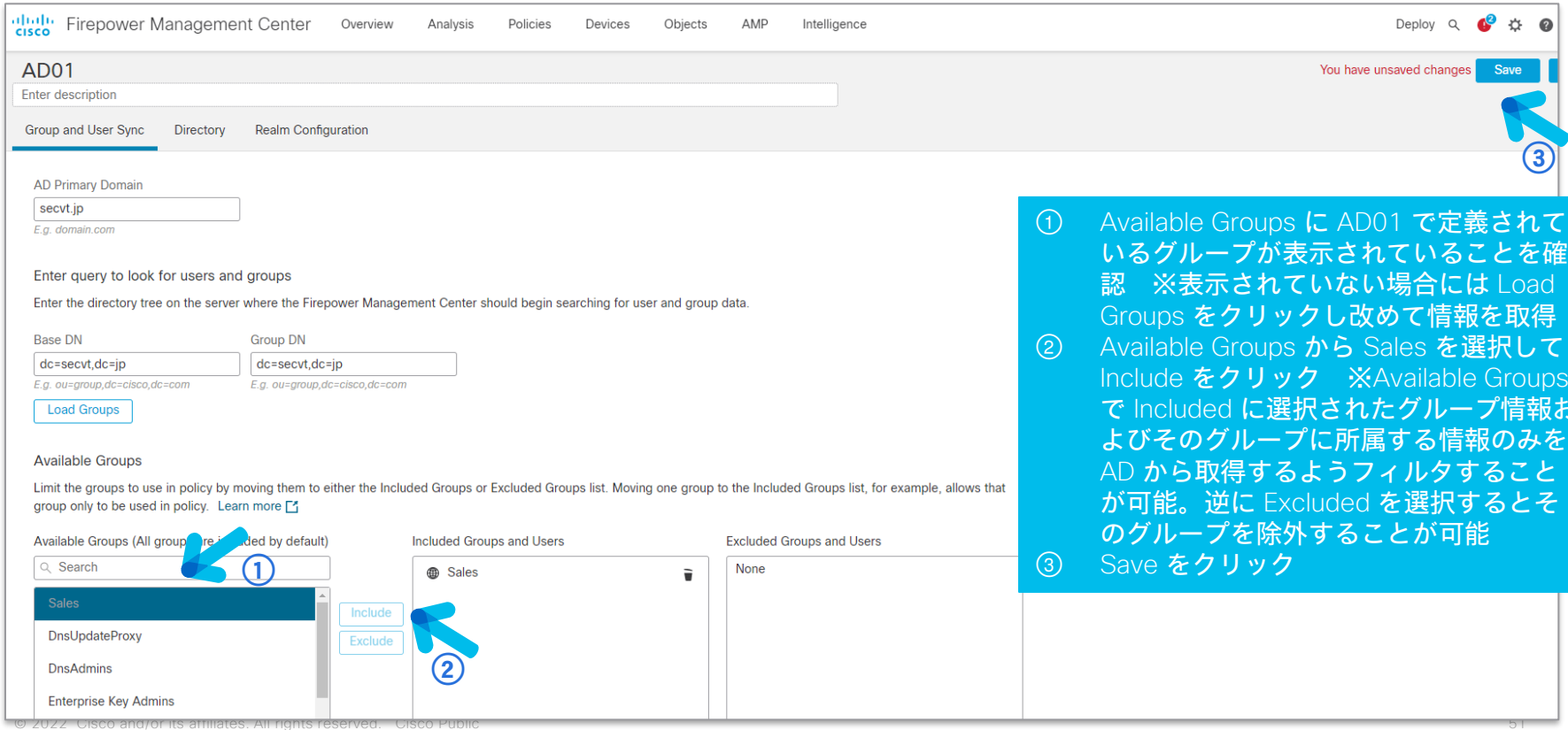
FMC での Realm（レルム）設定

- 選択したユーザーとグループを使ってポリシー設定を行うために FMC で AD Realm の作成を実施
  System > Integration > Realms



① Add Realm をクリック
② 任意の名前を入力
③ Type で AD を選択
④ AD Primary Domain で secvt.jp を入力
⑤ ディレクトリ参照用のユーザ名/パスワードを入力。ユーザ名は @ domain の形式
⑥ Base DN を入力
⑦ Directory Server Configuration に移動し、AD01 の IP アドレスを入力
⑧ Encryption を今回は None で設定
⑨ Resolve via route lookup を選択
⑩ Test をクリックし接続が成功することを確認
⑪ Configure Groups and Users をクリック

FMC での Realm（レルム）設定



① Available Groups に AD01 で定義されているグループが表示されていることを確認　※表示されていない場合には Load Groups をクリックし改めて情報を取得

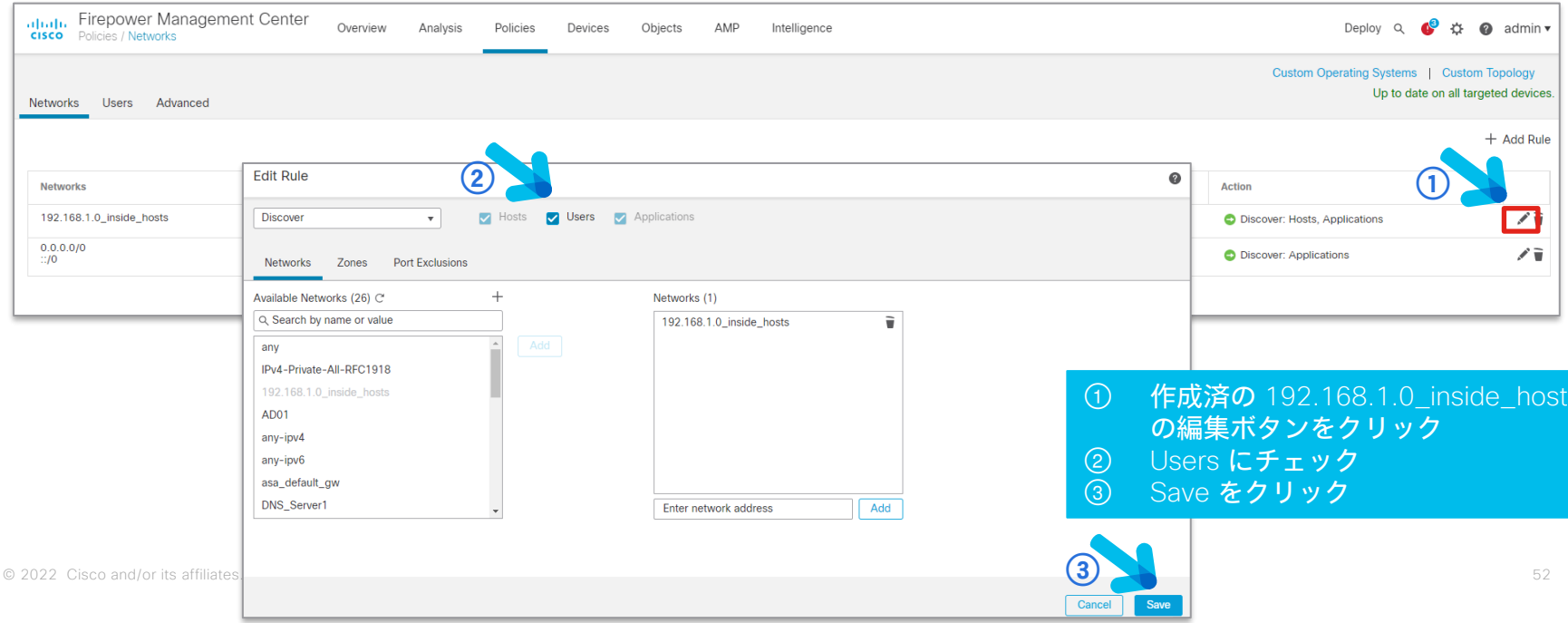
② Available Groups から Sales を選択して Include をクリック　※Available Groups で Included に選択されたグループ情報およびそのグループに所属する情報のみを AD から取得するようフィルタすることが可能。逆に Excluded を選択するとそのグループを除外することが可能

③ Save をクリック

Network Discovery での User の追加

- Identity Source の連携に伴い、作成済の Network Discovery Policy ルールにて Users を追加していなければこれを追加する

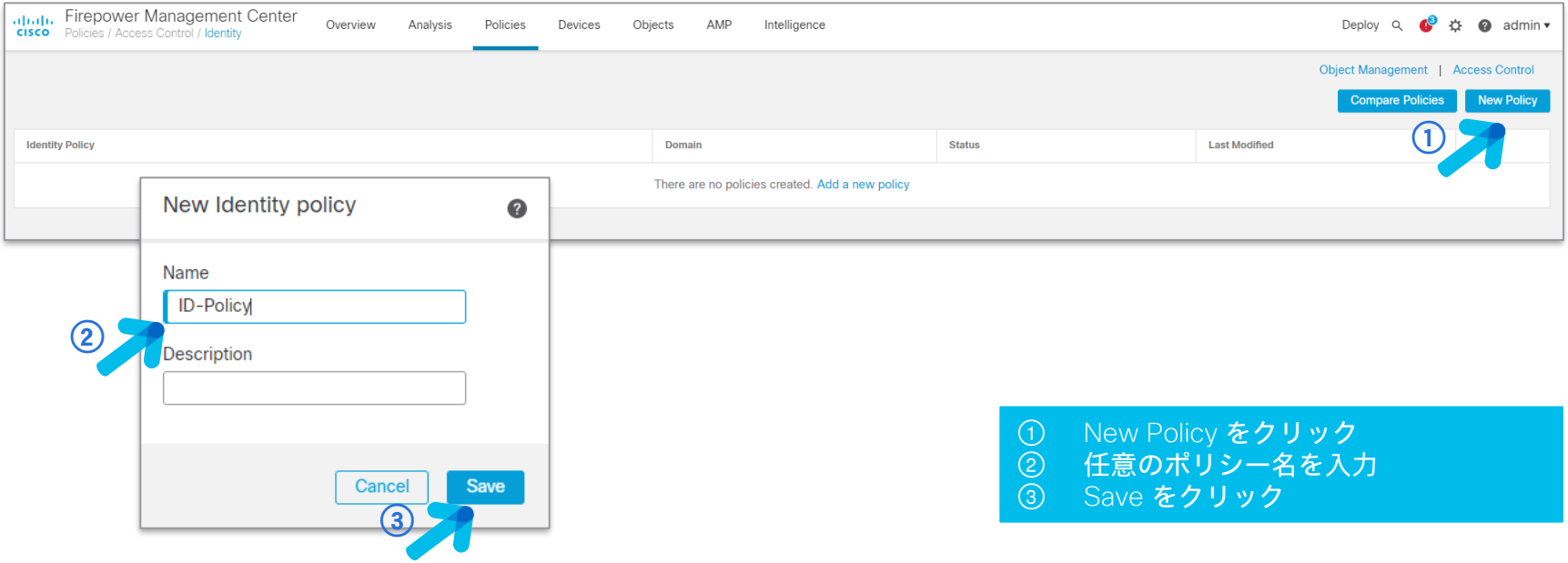
Policies > Network Discovery > Networks



Identity Policy の設定

- 新規に Identity Policy を作成する

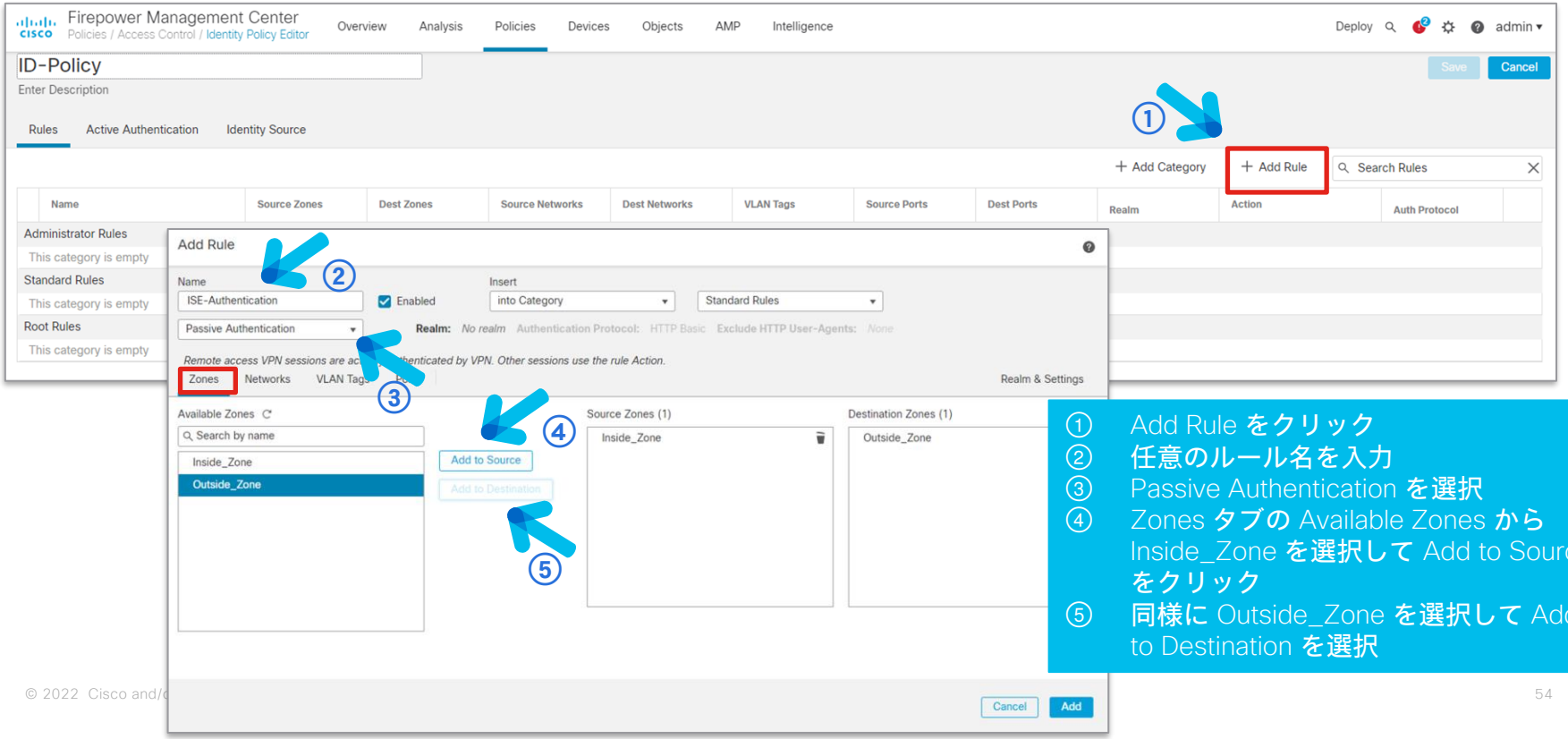
Policies > Access Control > Identity



① New Policy をクリック
② 任意のポリシー名を入力
③ Save をクリック

Identity Policy の設定

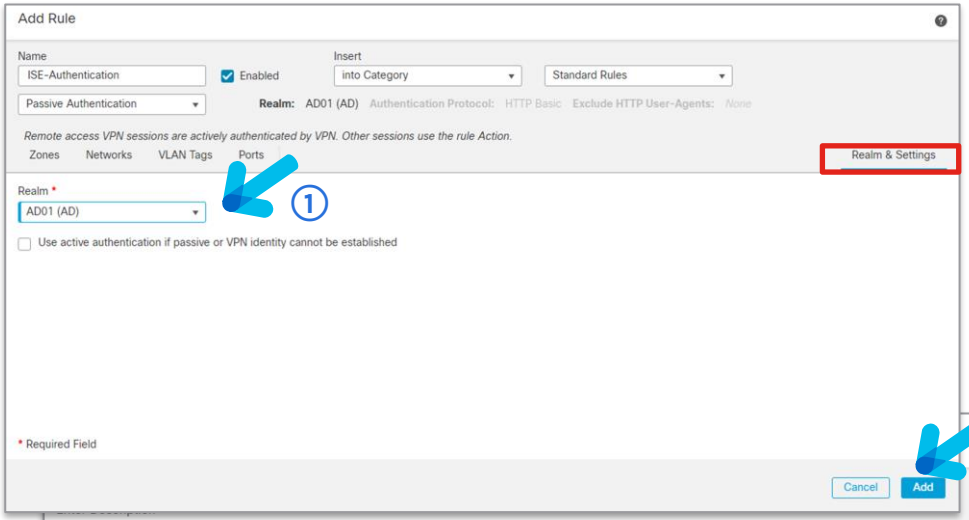
- 作成した Identity Policy にルールを追加する

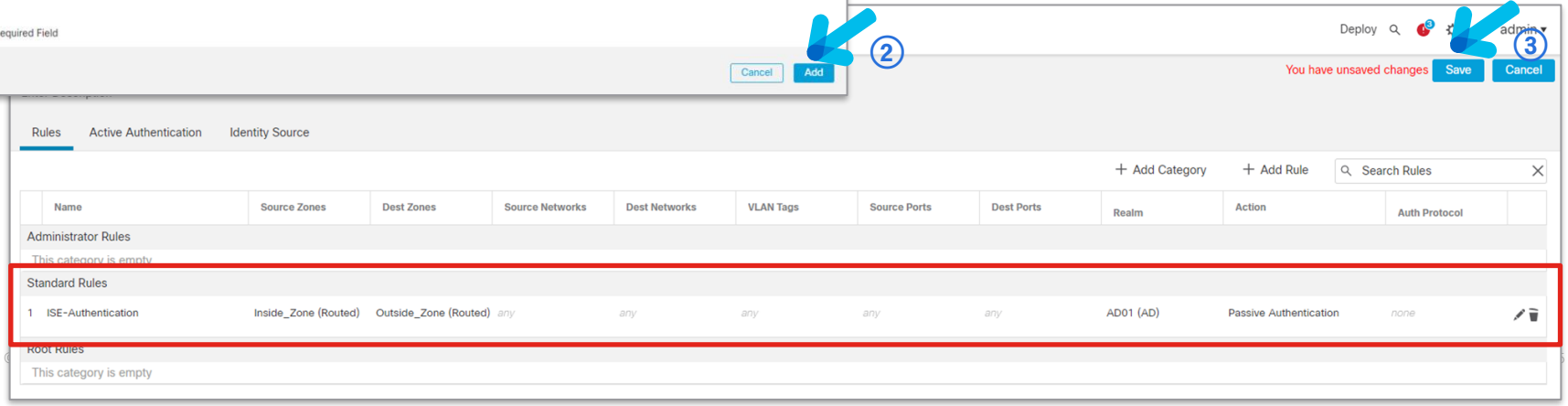


① Add Rule をクリック
② 任意のルール名を入力
③ Passive Authentication を選択
④ Zones タブの Available Zones から Inside_Zone を選択して Add to Source をクリック
⑤ 同様に Outside_Zone を選択して Add to Destination を選択

Identity Policy の設定

- 作成した Identity Policy にルールを追加する



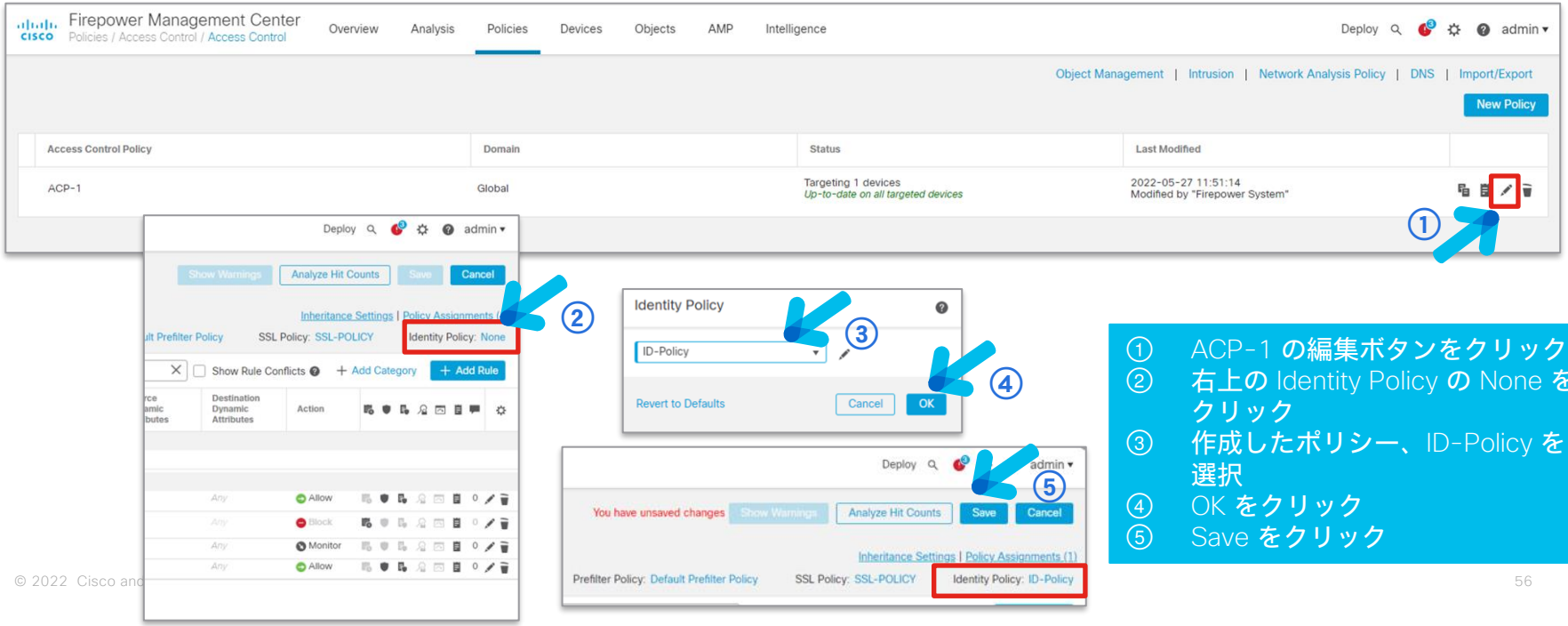


① Realm & Settings タブに移動し Realm で AD01 を選択
② Add をクリック
③ Save をクリック

ACP への Identity Policy の適用

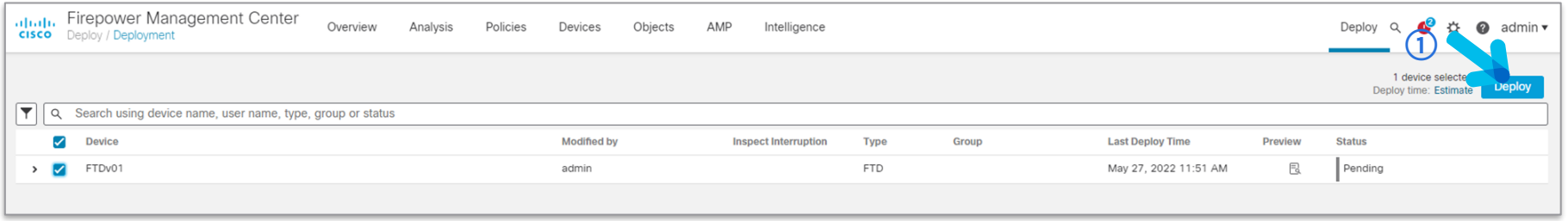
- 作成した Identity Policy を既存 ACP に適用する

Policies > Access Control > Access Control



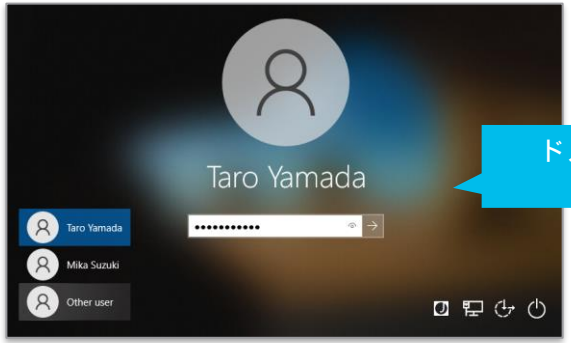
① ACP-1 の編集ボタンをクリック
② 右上の Identity Policy の None をクリック
③ 作成したポリシー、ID-Policy を選択
④ OK をクリック
⑤ Save をクリック

設定の FTD への展開

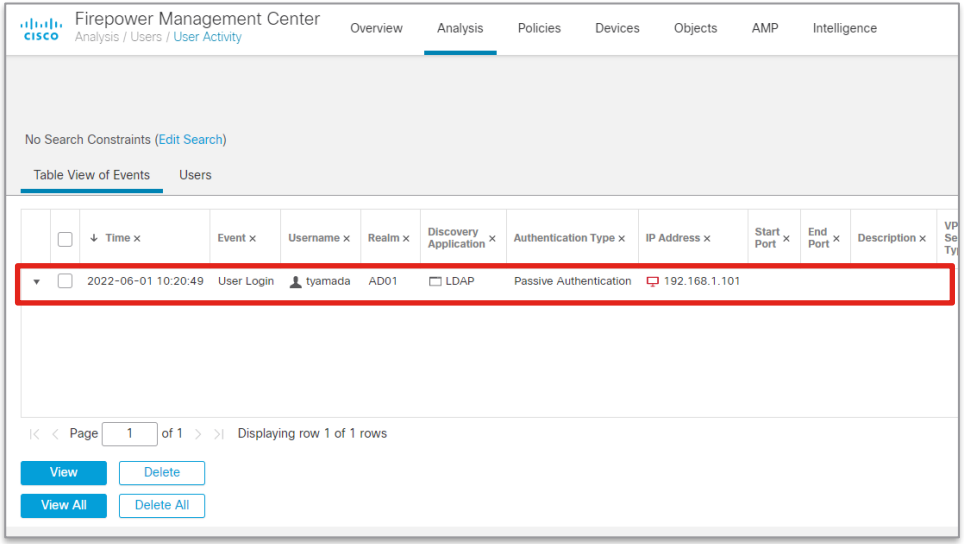


① Deploy をクリックして設定内容を FTDv01 に適用

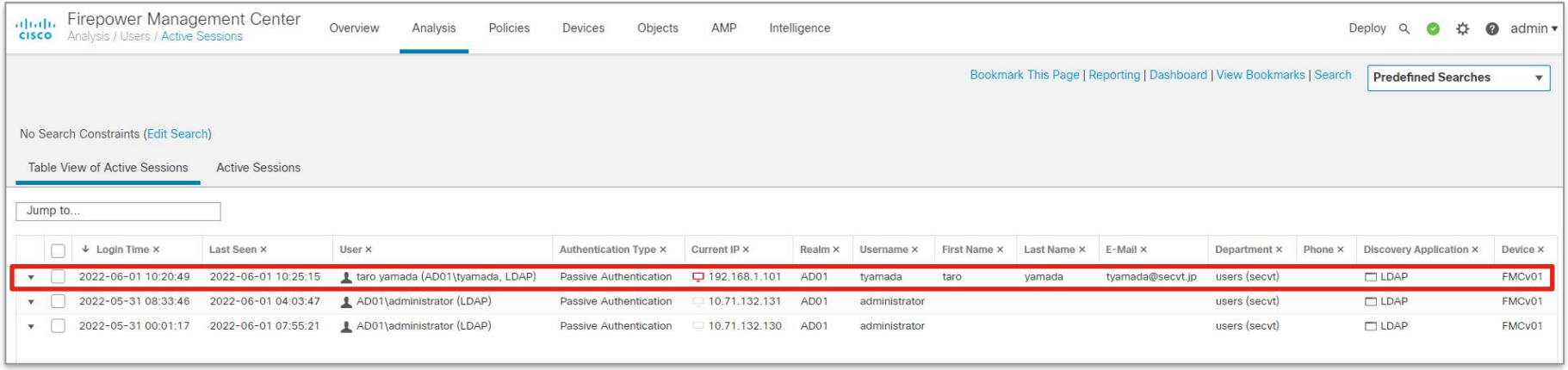
接続テスト＆Monitoring Events



- Analysis > Users > User Activities

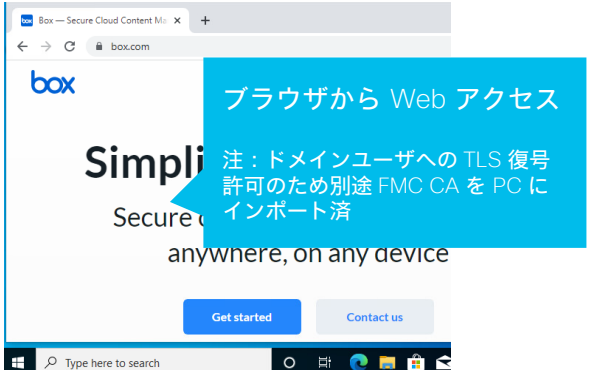


- Analysis > Users > Active Sessions



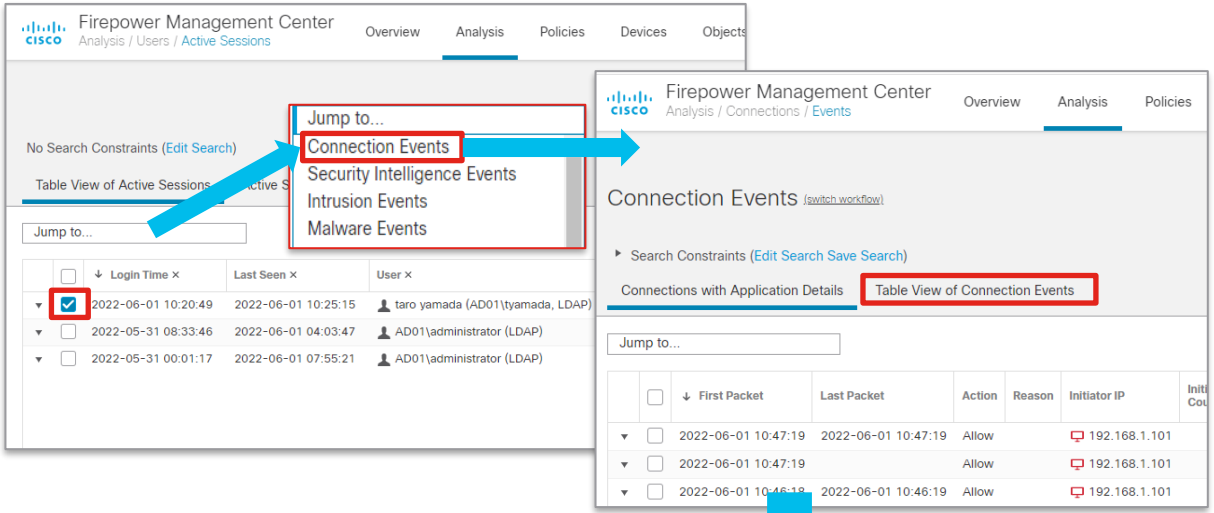
接続テスト &
Monitoring Events

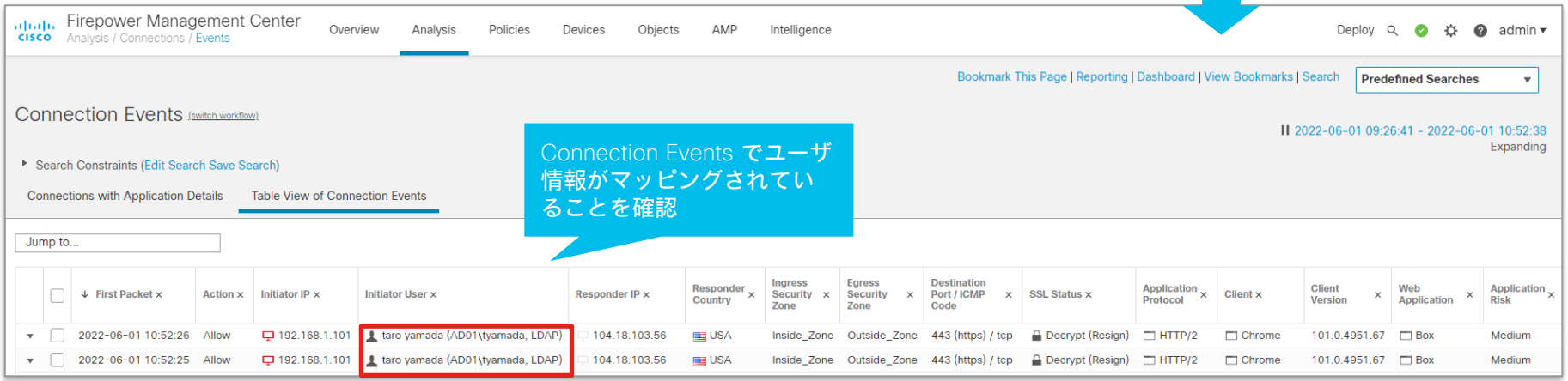
- Analysis > Users > Active Sessions



ブラウザから Web アクセス

注：ドメインユーザへの TLS 復号許可のため別途 FMC CA を PC にインポート済

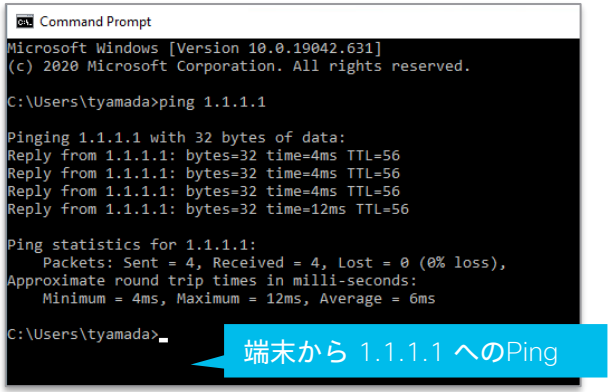


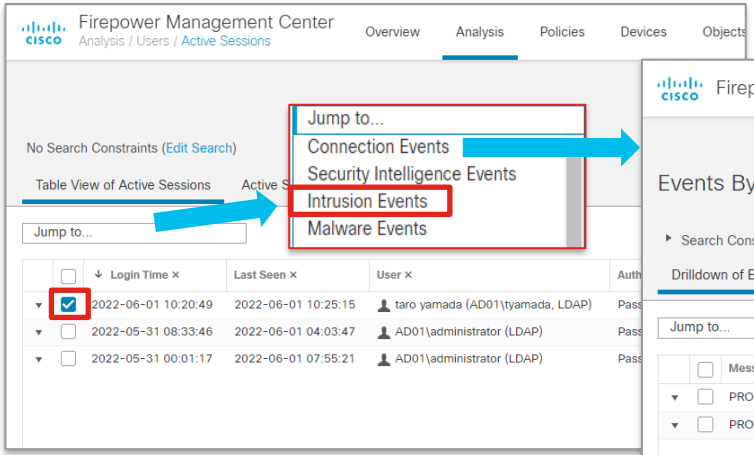


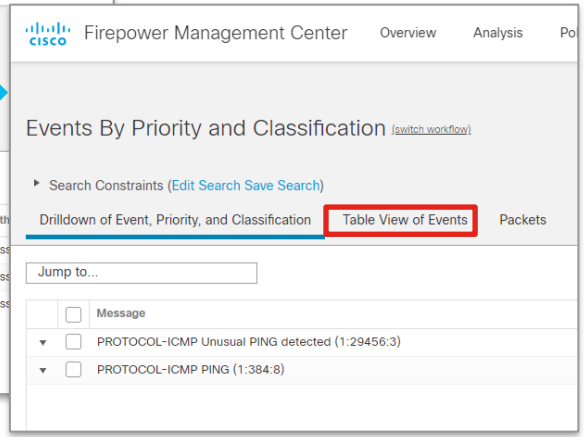
Connection Events でユーザ情報がマッピングされていることを確認

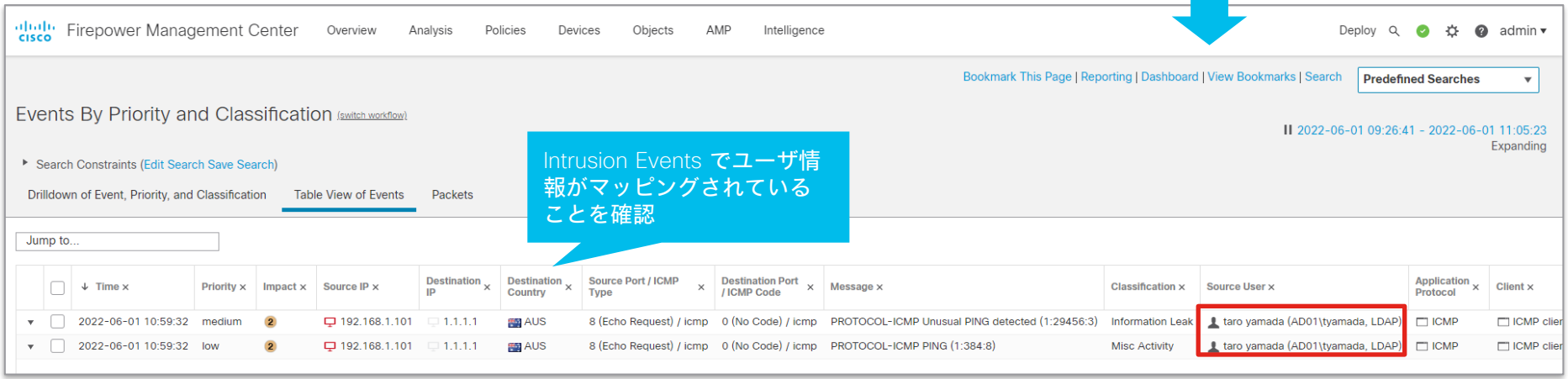
接続テスト&
Monitoring Events

- Analysis > Users > Active Sessions



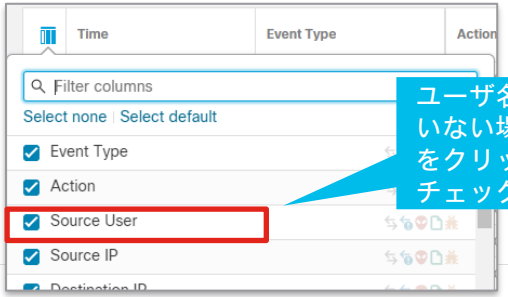






Monitoring Events

- Unified Events



Firepower Management Center
Analysis / Unified Events

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Deploy | admin

Refresh

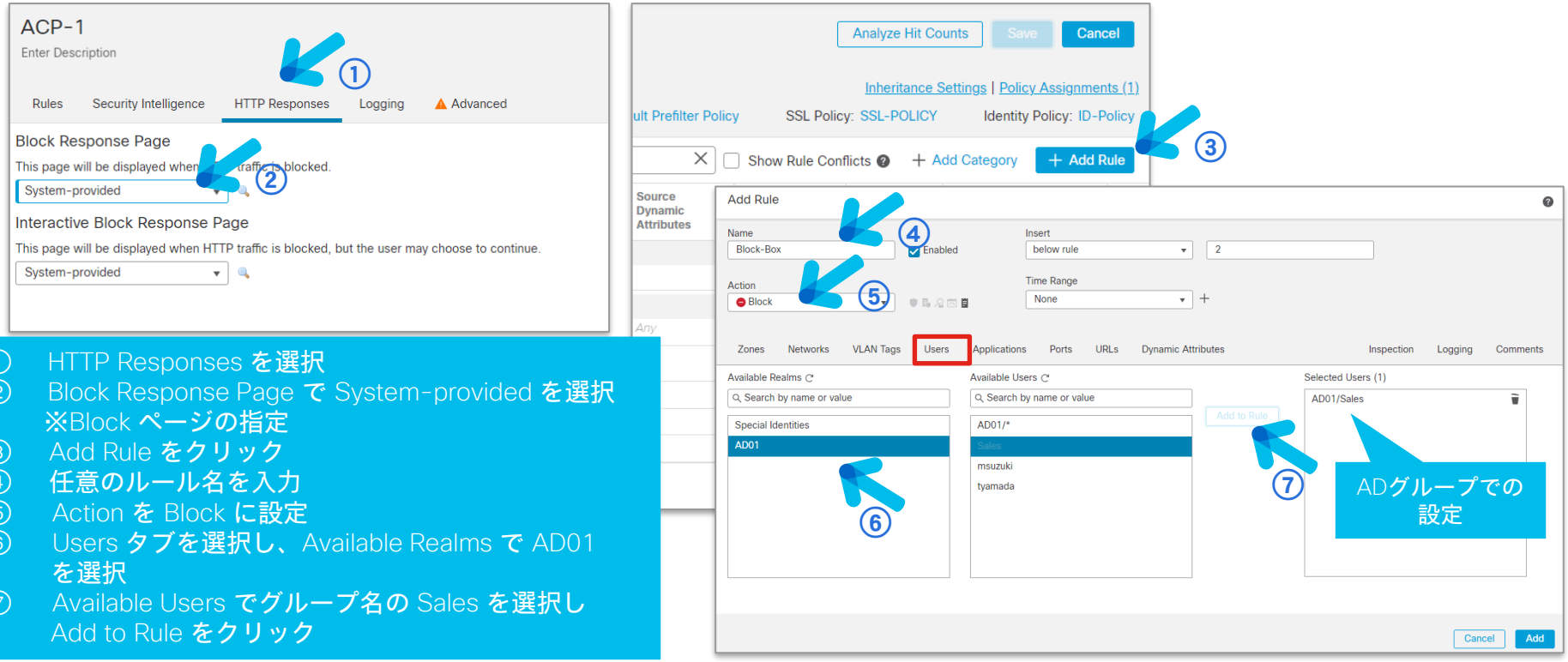
Showing all 1,510 events (1,464 2 44)

2022-06-01 10:07:28 JST → 2022-06-01 11:07:28 JST 1h | Go Live

Time	Event Type	Action	Source User	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Ac
2022-06-01 11:04:01	Connection	Monitor	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.119.249.228	53439 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR	AC
2022-06-01 11:04:01	Connection	Monitor	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.119.249.228	53438 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR	AC
2022-06-01 11:04:01	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53437 / tcp	443 (https) / tcp	Microsoft Windows Live S	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:04:00	Connection	Monitor	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.119.249.228	53436 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR	AC
2022-06-01 11:04:00	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53435 / tcp	443 (https) / tcp	Microsoft Windows Live S	URL-MONITOR, CATCH-ALL	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	104.46.162.226	53433 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53432 / tcp	443 (https) / tcp	Microsoft Windows Live S	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53431 / tcp	443 (https) / tcp	Microsoft Windows Live S	URL-MONITOR, CATCH-ALL	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53430 / tcp	443 (https) / tcp	Microsoft Windows Live S	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:03:34	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	52.139.250.253	53429 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:03:33	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.90.189.152	53428 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:32	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	1.1.1.1	8 (Echo Request)	0 (No Code) / icr		CATCH-ALL	AC
2022-06-01 10:59:32	Intrusion	Pass	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	1.1.1.1	8 (Echo Request)	0 (No Code) / icr		CATCH-ALL	AC
2022-06-01 10:59:32	Intrusion	Pass	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	1.1.1.1	8 (Echo Request)	0 (No Code) / icr		CATCH-ALL	AC
2022-06-01 10:59:29	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	52.139.154.55	53427 / tcp	443 (https) / tcp	NBC News	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:29	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	52.139.154.55	53426 / tcp	443 (https) / tcp	NBC News	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:25	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	13.107.246.254	53425 / tcp	443 (https) / tcp	Bing	URL-MONITOR, CATCH-ALL	AC
2022-06-01 10:59:25	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	117.18.232.200	53424 / tcp	443 (https) / tcp	Bing	CATCH-ALL	AC
2022-06-01 10:59:25	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	210.57.94.192	53423 / tcp	443 (https) / tcp	Office 365	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:23	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.90.184.73	53422 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR, CATCH-ALL	AC

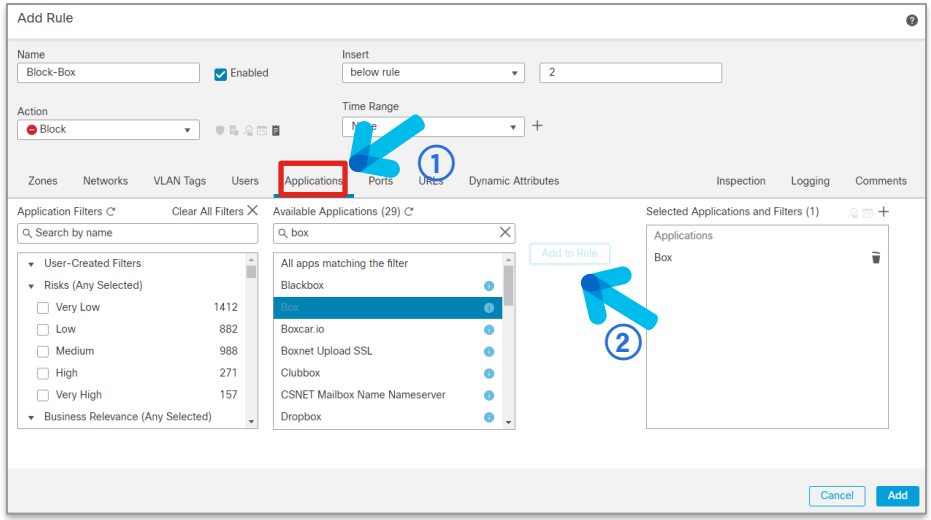
参考：ユーザ・グループベースの ACP ルール設定

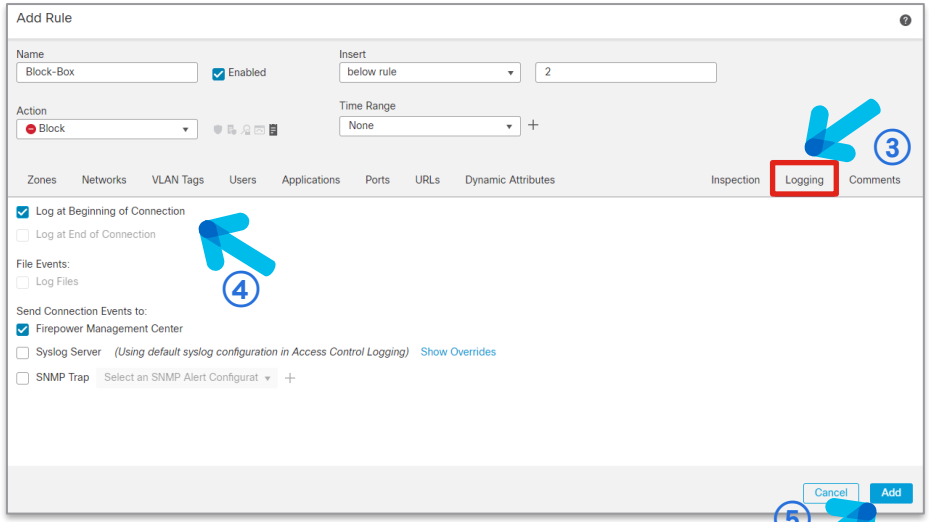
- Policies > Access Control > Access Control



① HTTP Responses を選択
② Block Response Page で System-provided を選択
※Block ページの指定
③ Add Rule をクリック
④ 任意のルール名を入力
⑤ Action を Block に設定
⑥ Users タブを選択し、Available Realms で AD01 を選択
⑦ Available Users でグループ名の Sales を選択し Add to Rule をクリック

参考：ユーザ・グループベースの ACP ルール設定





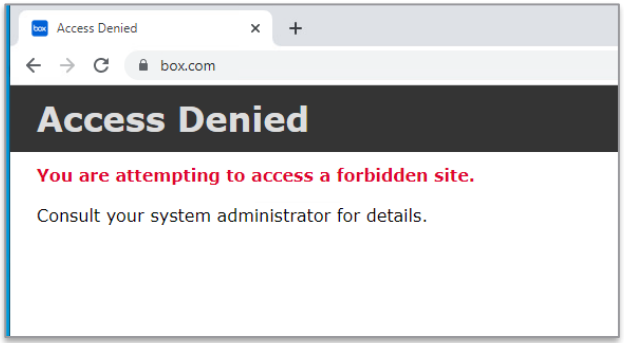
1	RAVPN-Access	Outside_Zone	Any	VPN-Pool-IPs	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
2	TIME-BASED (Disabled)	Any	Any	OFFICE	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block
3	Block-Box	Any	Any	Any	Any	Any	AD01/Sales	Box	Any	Any	Any	Any	Any	Block
4	URL-MONITOR	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any (Except Unc	Any	Any	Monitor
5	CATCH-ALL	Any	Any	Any										

① Applications タブを選択
② Available Applications から Box を検索して選択し、Add to Rule を選択
③ Logging に移動
④ Log at Beginning Connection をチェック
⑤ Add をクリックして、Save → Deploy

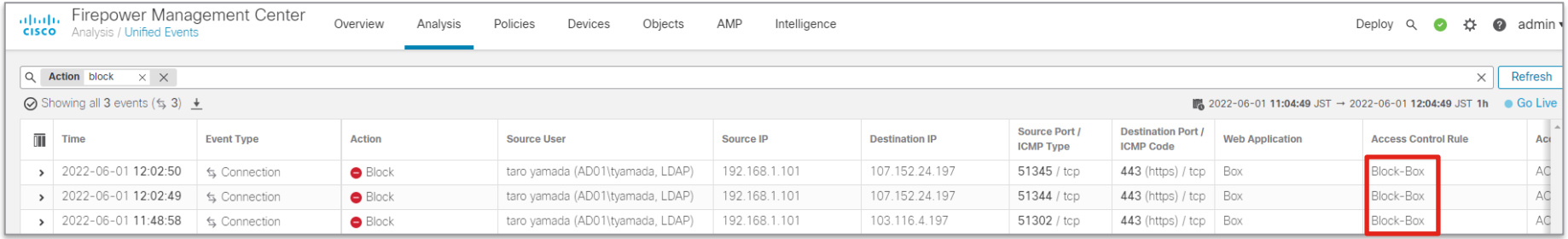
参考：ユーザ・グループベースの ACP ルール設定

- 接続テスト & Monitoring Events

  Sales グループに属する Taro Yamada のアクセス



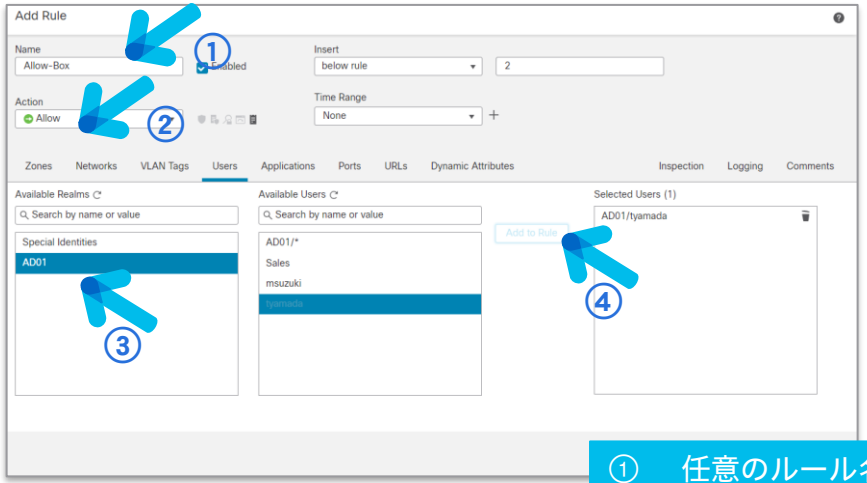
- Unified Events

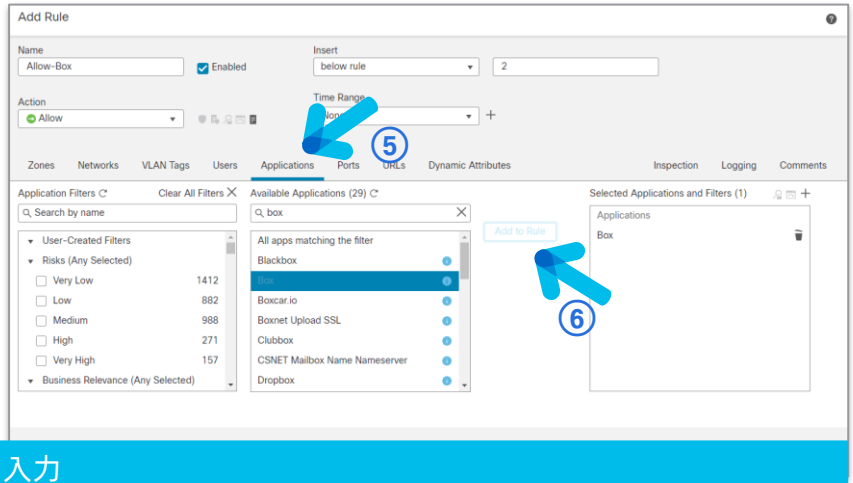


参考：ユーザ・グループベースの ACP ルール設定

- Sales グループでは Block だが Taro Yamada のみ例外設定追加

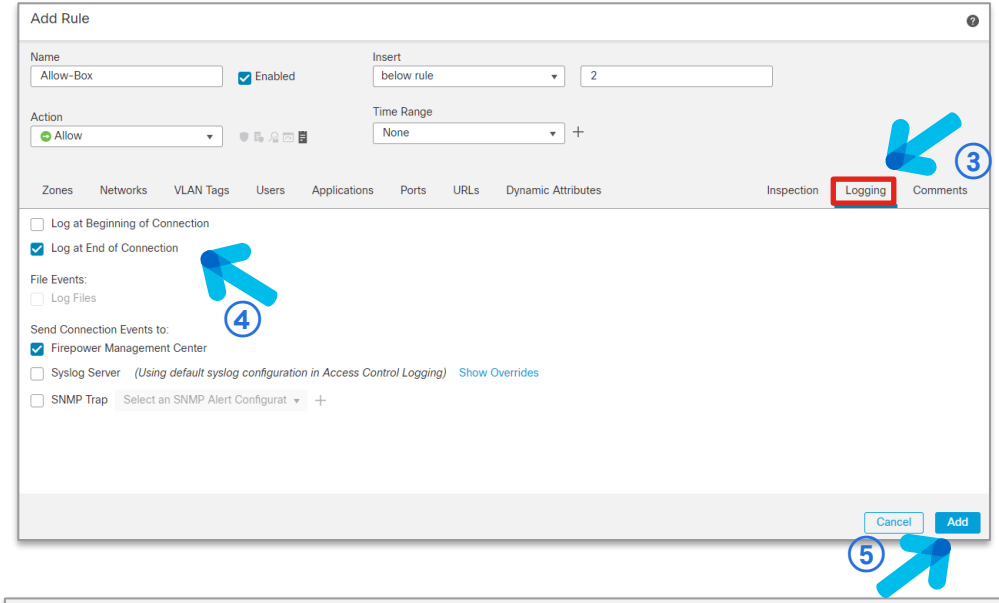
Policies > Access Control > Access Control > ACP-1 編集 > Add Rule



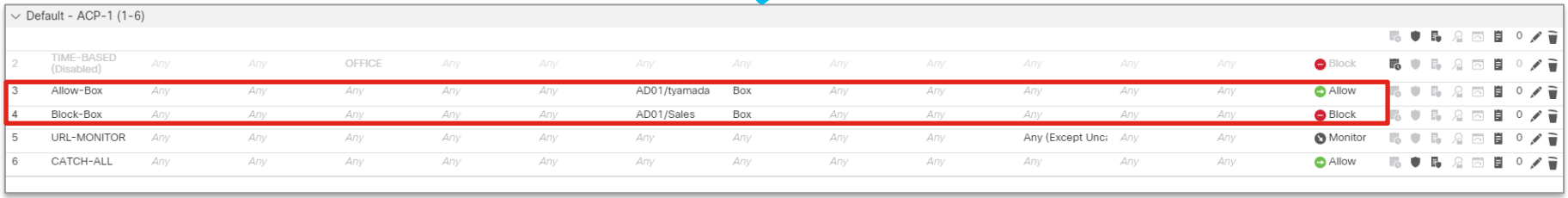


① 任意のルール名を入力
② Action で Allow を選択
③ Users タブに移動し、Available Realms で AD01 を選択
④ Available Users で tyamadaを選択し、Add to Rule をクリック
⑤ Applications タブを選択
⑥ Available Applications でBoxを検索して選択し、Add to Rule をクリック

参考：ユーザ・グループベースの ACP ルール設定



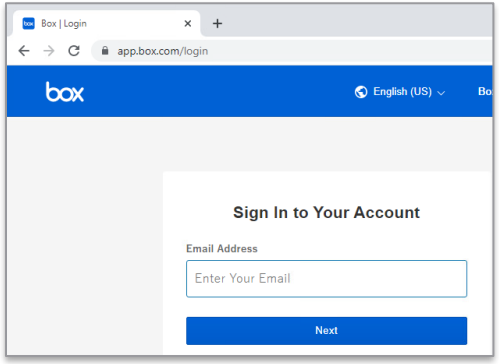
① Logging を選択
② Log at Beginning Connection をチェック
③ Add をクリックして、Save → Deploy



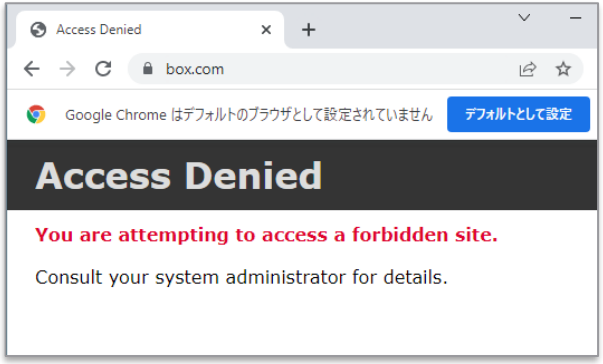
参考：ユーザ・グループベースの ACP ルール設定

- 接続テスト & Monitoring Events

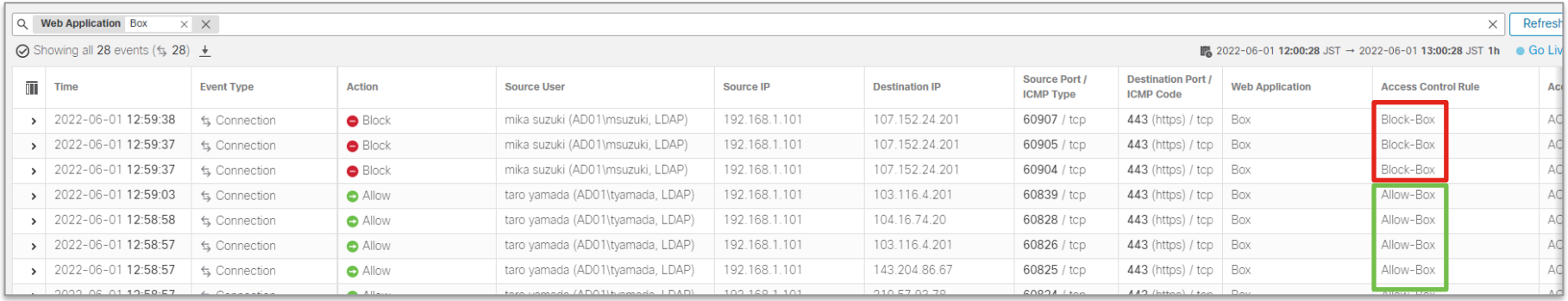
Sales グループに属する Taro Yamada のアクセス



Sales グループに属する Mika Suzuki のアクセス



- Unified Events



Web Application Box

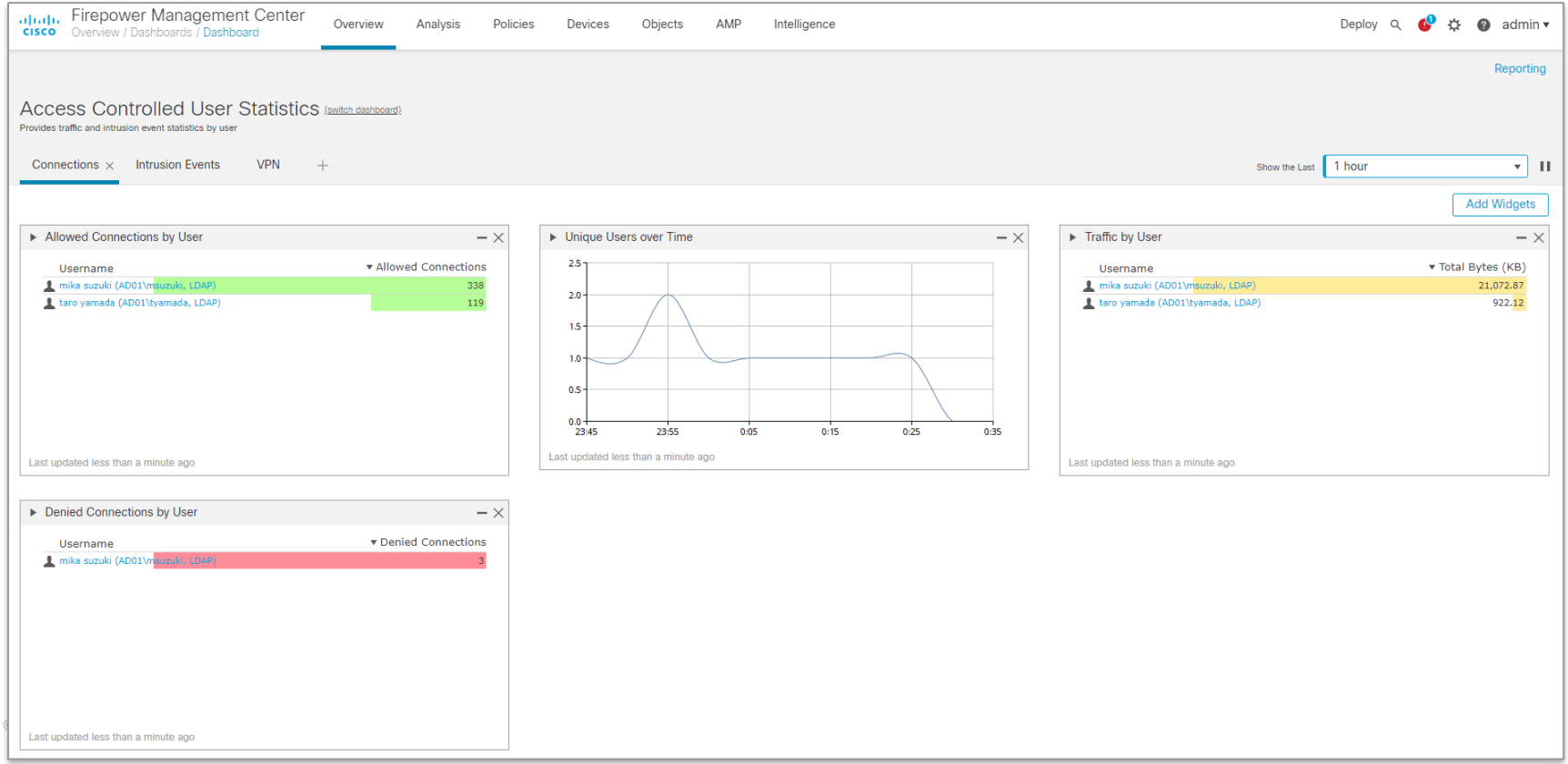
Showing all 28 events (28)

2022-06-01 12:00:28 JST → 2022-06-01 13:00:28 JST 1h

Time	Event Type	Action	Source User	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule
2022-06-01 12:59:38	Connection	Block	mika suzuki (AD01\msuzuki, LDAP)	192.168.1.101	107.152.24.201	60907 / tcp	443 (https) / tcp	Box	Block-Box
2022-06-01 12:59:37	Connection	Block	mika suzuki (AD01\msuzuki, LDAP)	192.168.1.101	107.152.24.201	60905 / tcp	443 (https) / tcp	Box	Block-Box
2022-06-01 12:59:37	Connection	Block	mika suzuki (AD01\msuzuki, LDAP)	192.168.1.101	107.152.24.201	60904 / tcp	443 (https) / tcp	Box	Block-Box
2022-06-01 12:59:03	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	103.116.4.201	60839 / tcp	443 (https) / tcp	Box	Allow-Box
2022-06-01 12:58:58	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	104.16.74.20	60828 / tcp	443 (https) / tcp	Box	Allow-Box
2022-06-01 12:58:57	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	103.116.4.201	60826 / tcp	443 (https) / tcp	Box	Allow-Box
2022-06-01 12:58:57	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	143.204.86.67	60825 / tcp	443 (https) / tcp	Box	Allow-Box

Monitoring Events

- Overview > switch dashboard > Access Controlled User Statistics



13. AnyConnect VPN 接続の設定

FTD におけるリモートアクセス VPN

- ASA と同様に AnyConnect Client を利用したリモートアクセス VPN をサポート (TLS/DTLS, および IKEv2)
- FTD 7.0 (FMC 利用) で新たにサポートされた機能は以下の通り
  - Dynamic Access Policy (DAP)
  - AnyConnect カスタムアトリビュート
    - Per App VPN for mobile device, Dynamic Split-Tunneling, AnyConnect Defer Update
  - SAML 認可 (SAML 認証は FTD 6.7 より利用可)
  - ローカルユーザ認証
  - マルチ証明書認証
  - リモートアクセス VPN ロードバランシング

詳細はリリースノートを参照

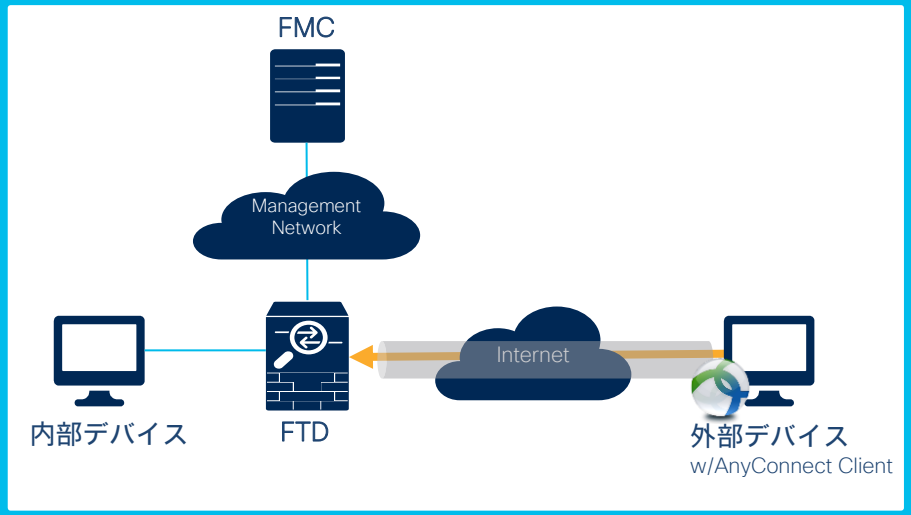
参考) FTD7.0 (FMC 利用) でサポートされていない機能

- Clientless VPN
- AnyConnect VPN SAML external browser (FTD 7.1 で利用可)
- AnyConnect customization
- AnyConnect scripts
- AnyConnect localization
- SCEP proxy
- WSA integration
- TACACS, Kerberos

本セットアップガイドでの設定条件

- VPN フルトンネル接続
- SSL (TLS/DTLS) での接続
- VPN プールアドレスは内部ネットワークアドレス (192.168.1.0/24) と同じネットワークで定義
- Local DB を作成して Local 認証を実施

  ※12章で作成した AD レルムを利用することも可能だが、今回は 7.0 の新機能である Local 認証をテストする
- 自己証明書を作成・使用
  - Wizard での VPN ポリシー設定で ID Certificate の指定が必要なため
- VPN 通信にも Intrusion Policy、および File Policy を適用



FMC での設定ステップ

1. AnyConnect ライセンスの適用
2. AnyConnect Client のインポート
3. VPN Pool の設定
4. ID Certificate の設定
5. Local DB の設定
6. Wizard を使用したリモートアクセス VPN ポリシーの設定
7. リモートアクセス用の ACP ルール設定
8. リモートアクセス用の NAT 除外ルール設定
9. FTD への設定の Deploy
10. 端末からの接続テスト

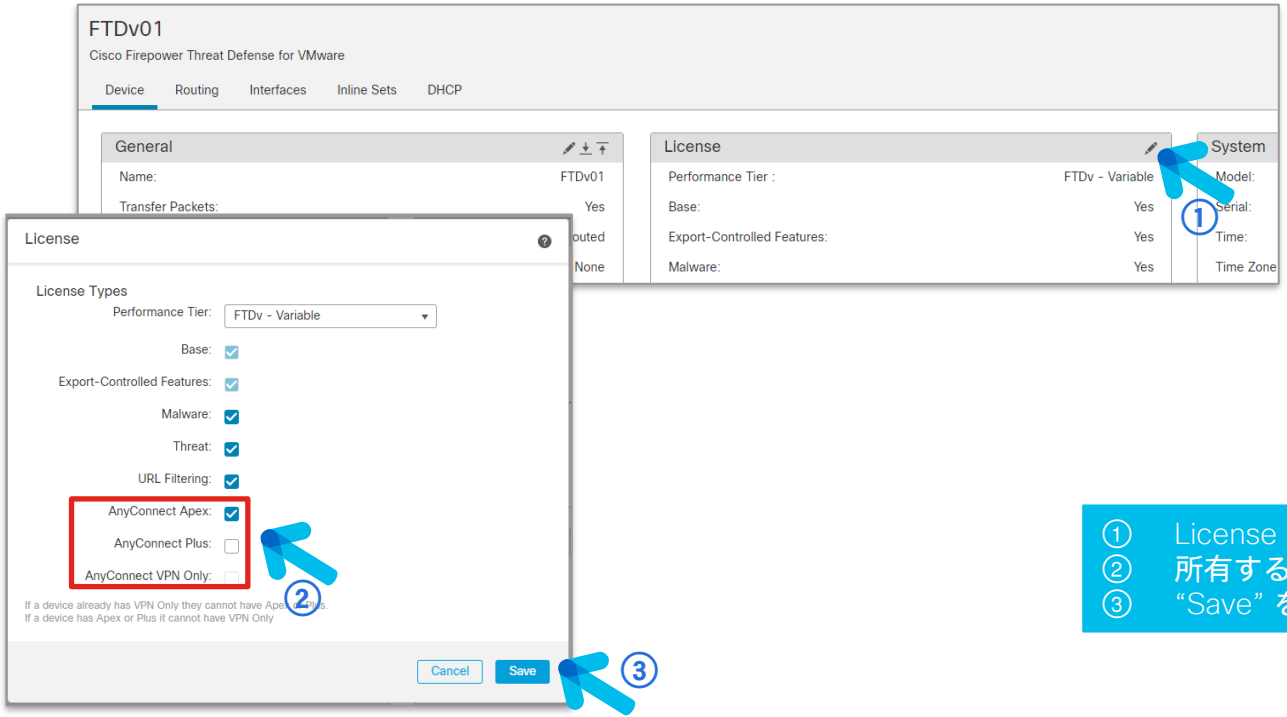
FTD における AnyConnect ライセンス

- FTD リモートアクセス VPN 利用にあたり、以下のいずれかのスマートライセンストークンが必要
  - AnyConnect VPN-only
  - AnyConnect Plus
  - AnyConnect Apex
- ライセンスが適用されていない限りリモートアクセス VPN の設定の FTD へのデプロイは不可

※スマートライセンス適用方法については Vol.1 「4. スマートライセンスの適用」の章を参照

AnyConnect ライセンスの適用

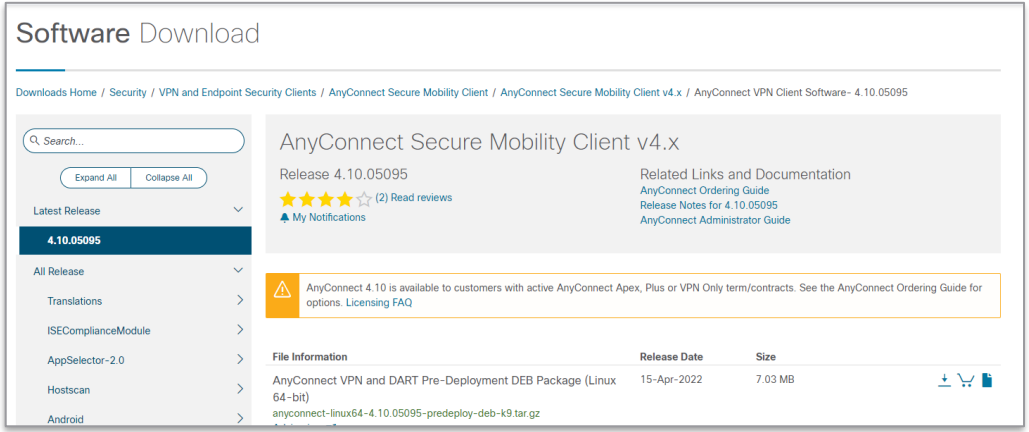
- 利用する FTD デバイスへのライセンスのアサイン
  Devices > Device Management > FTDv01 の Edit > Device タブ



① License の Edit ボタンをクリック
② 所有する AnyConnect ライセンスを選択
③ “Save” をクリック

AnyConnect Client のインポート

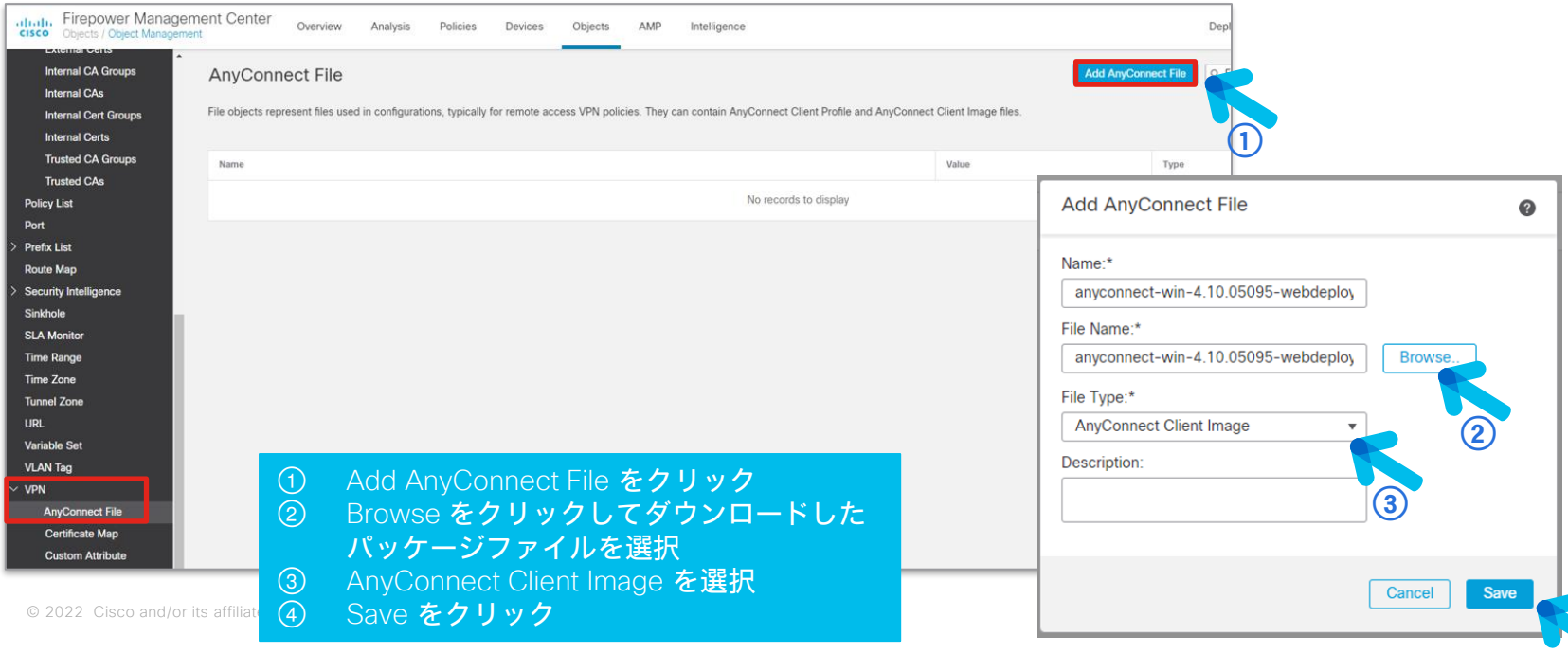
- Software Download サイトより AnyConnect Client ソフトウェアをダウンロード
  - https://software.cisco.com/download/home
  - AnyConnect Headend Deployment Package を選択
    - anyconnect-win-4.10.XXXX-webdeploy-k9.pkg



AnyConnect Client のインポート

- ダウンロードしたパッケージファイルの FMC へのインポート

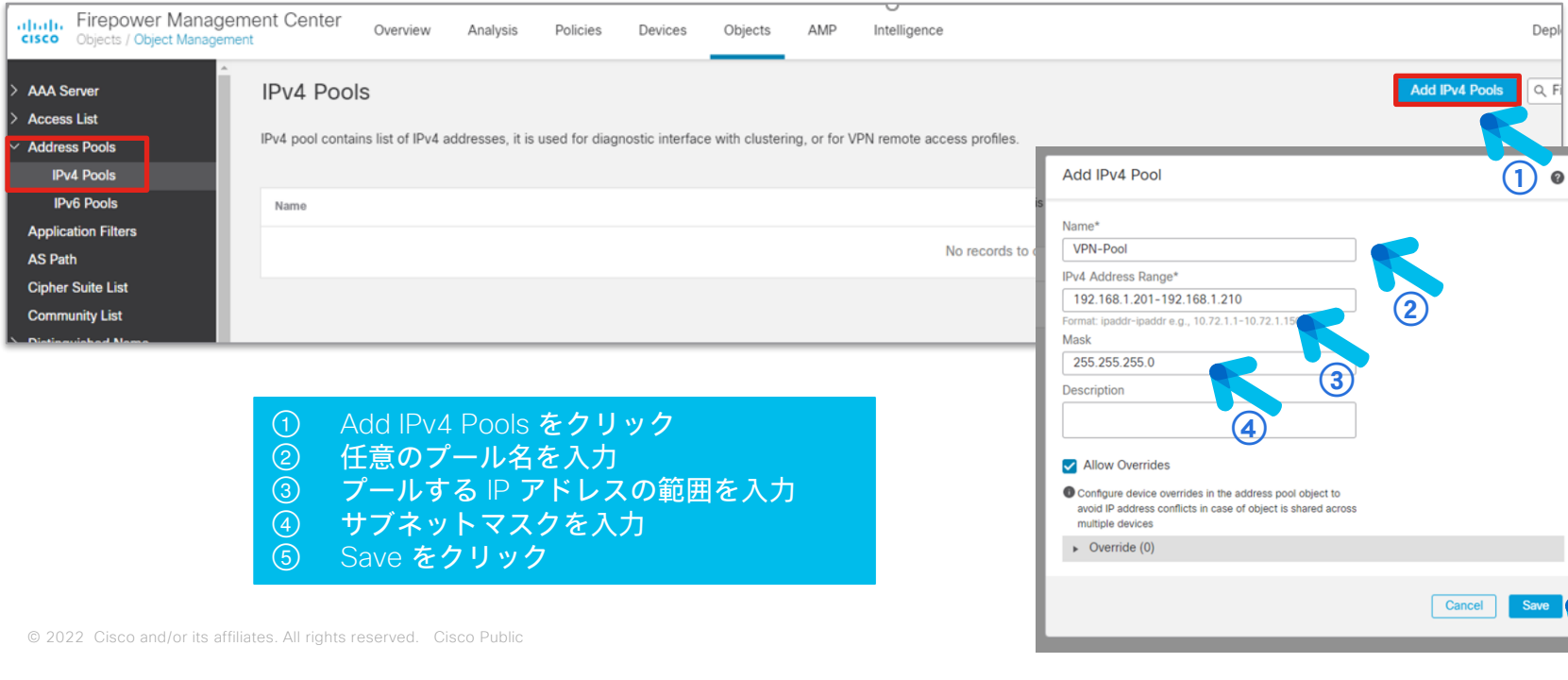
  Objects > Object Management > VPN > AnyConnect File



① Add AnyConnect File をクリック
② Browse をクリックしてダウンロードしたパッケージファイルを選択
③ AnyConnect Client Image を選択
④ Save をクリック

VPN Pool アドレスの設定

- Objects > Object Management > Address Pools > IPv4 Pools

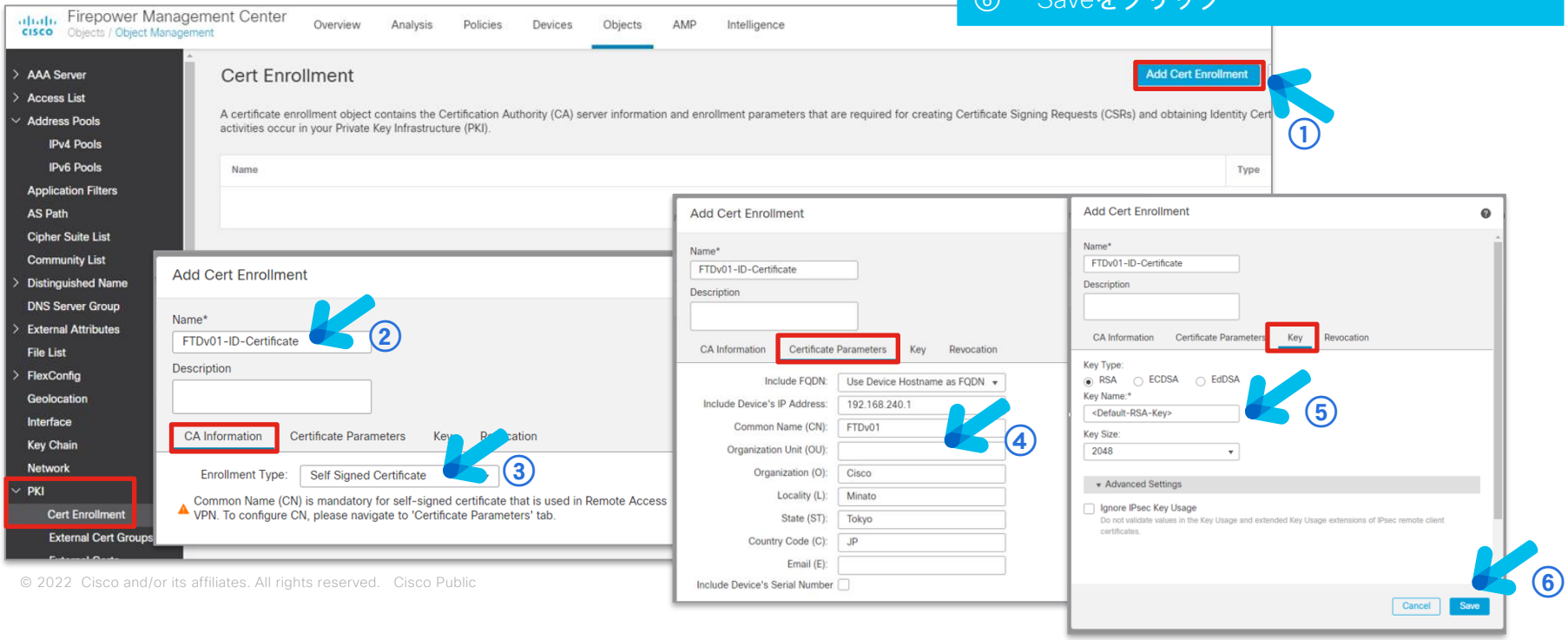


① Add IPv4 Pools をクリック
② 任意のプール名を入力
③ プールする IP アドレスの範囲を入力
④ サブネットマスクを入力
⑤ Save をクリック

ID Certificate の設定

- 自己証明書の生成と登録
  Objects > Object Management > PKI > Cert Enrollment

① Add Cert Enrollment をクリック
② 任意の証明書名を入力
③ CA Information タブを選択し、Enrollment Type で Self Signed Certificateを選択
④ Certificate Parameters タブを選択し、パラメータを入力 (CNはマスト)
⑤ Key タブを選択し必要に応じてKeyを生成 (今回は Default-RSA-Key を利用)
⑥ Saveをクリック

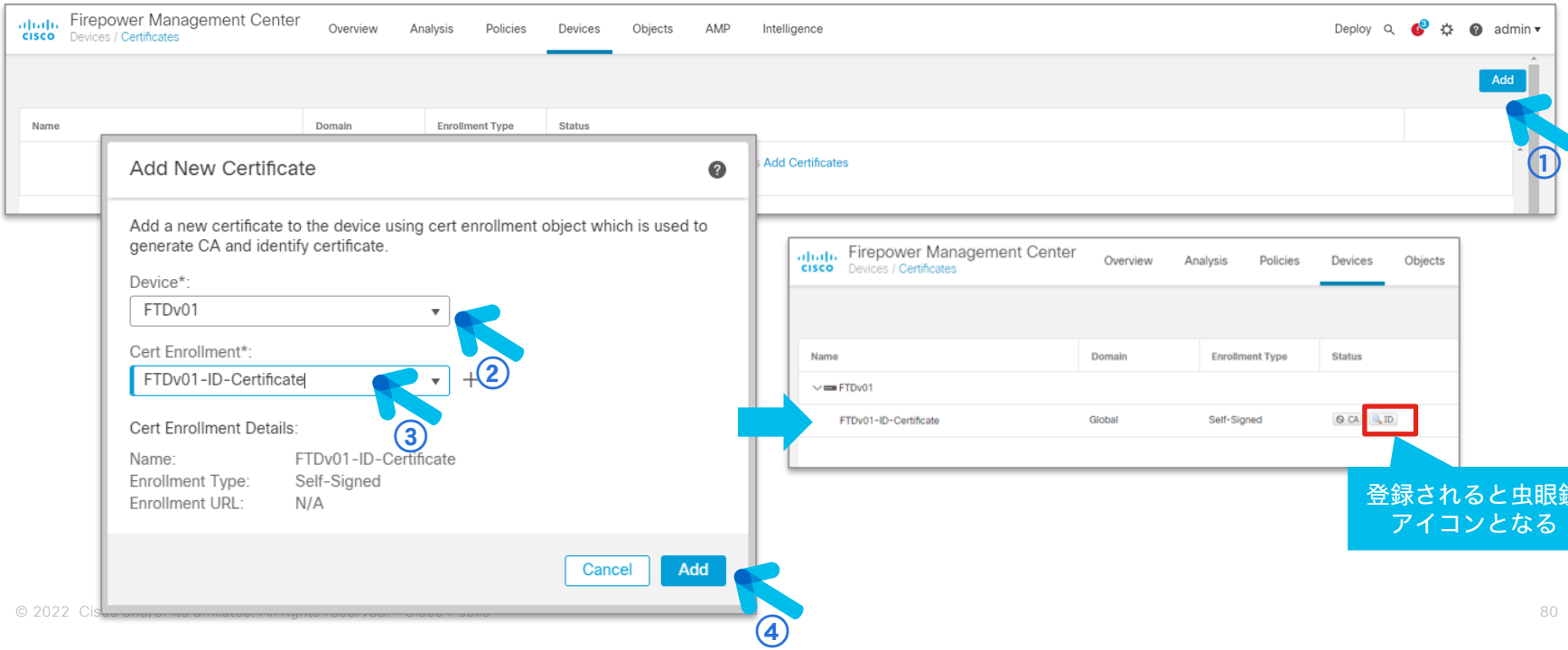


ID Certificate の設定

- FTD デバイスへの ID Certificate の登録

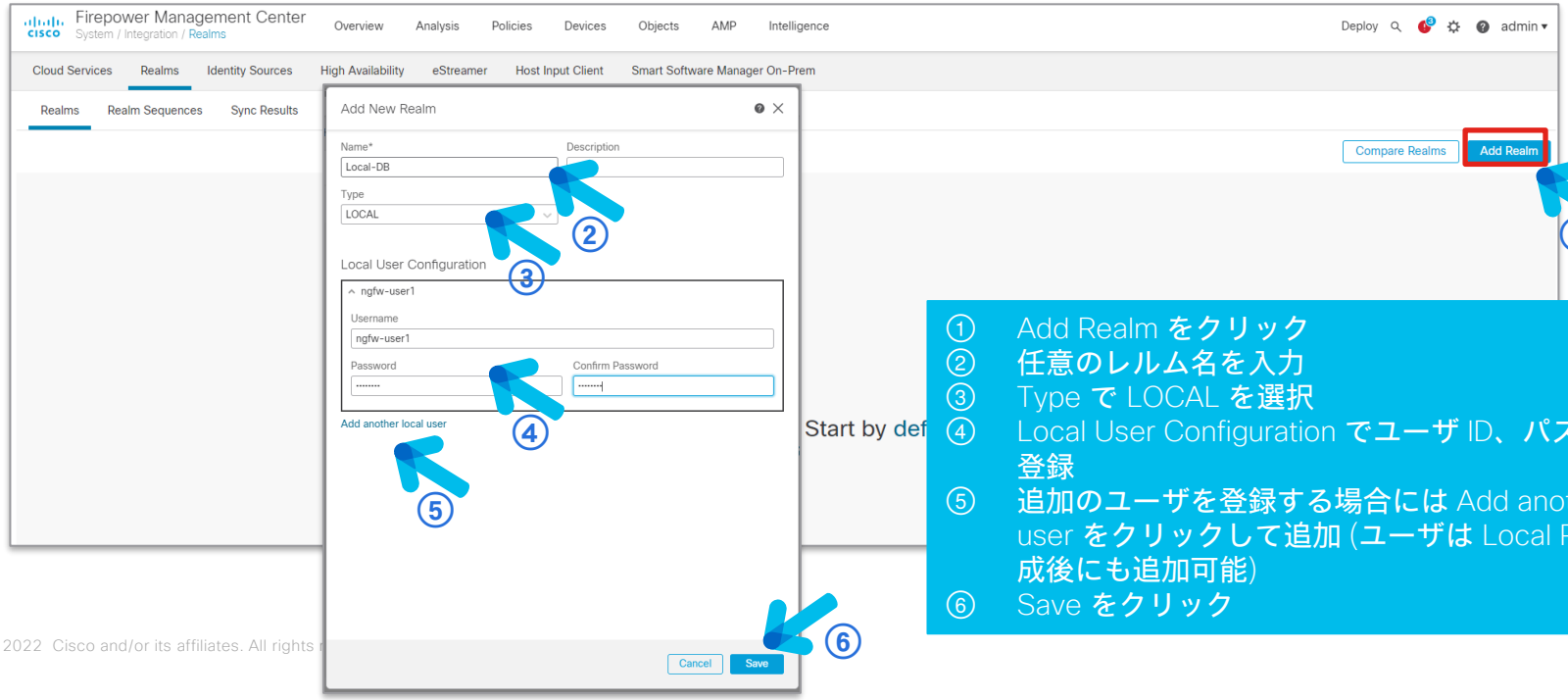
  Devices > Certificates

① Add をクリック
② 任意のデバイス名を入力
③ 作成した FTDv01-ID-Certificate を選択
④ Add をクリック



Local DB の設定

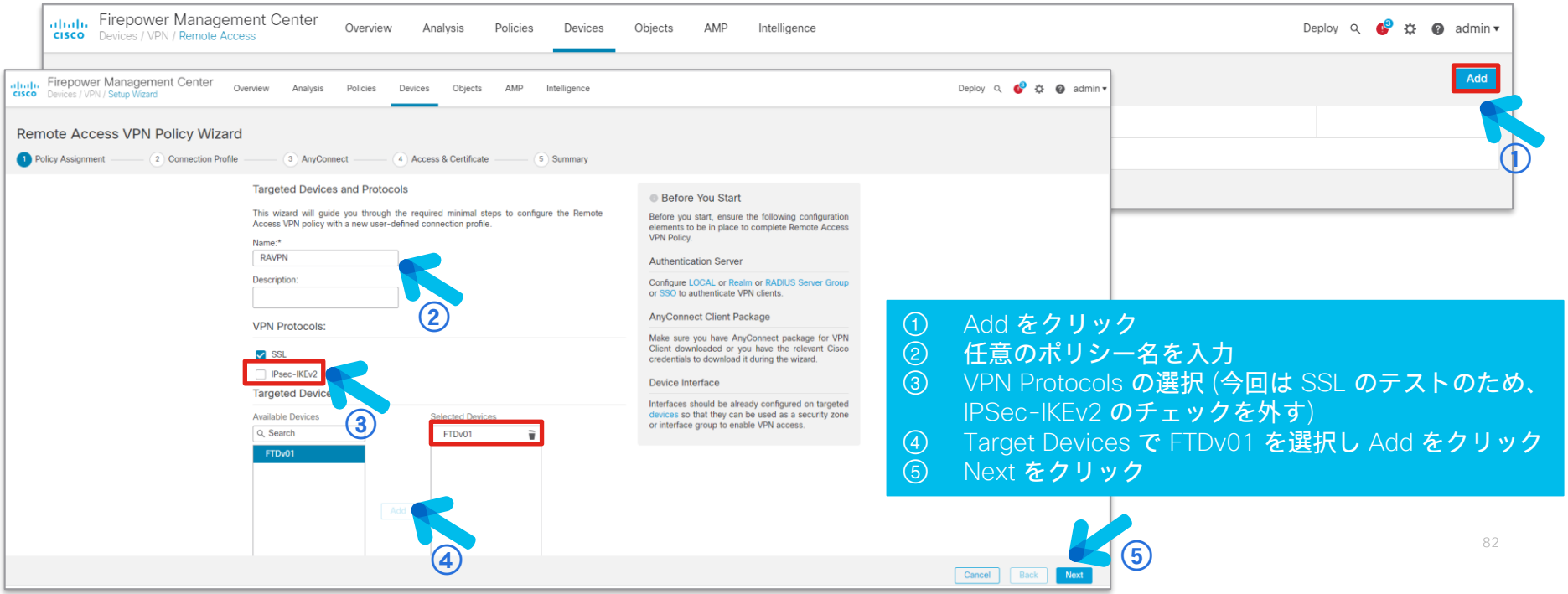
- 今回認証には Local DB を利用するため、Local DB の設定を実施
  System > Integration > Realms



① Add Realm をクリック
② 任意のレルム名を入力
③ Type で LOCAL を選択
④ Local User Configuration でユーザ ID、パスワードを登録
⑤ 追加のユーザを登録する場合には Add another local user をクリックして追加 (ユーザは Local Realm 作成後にも追加可能)
⑥ Save をクリック

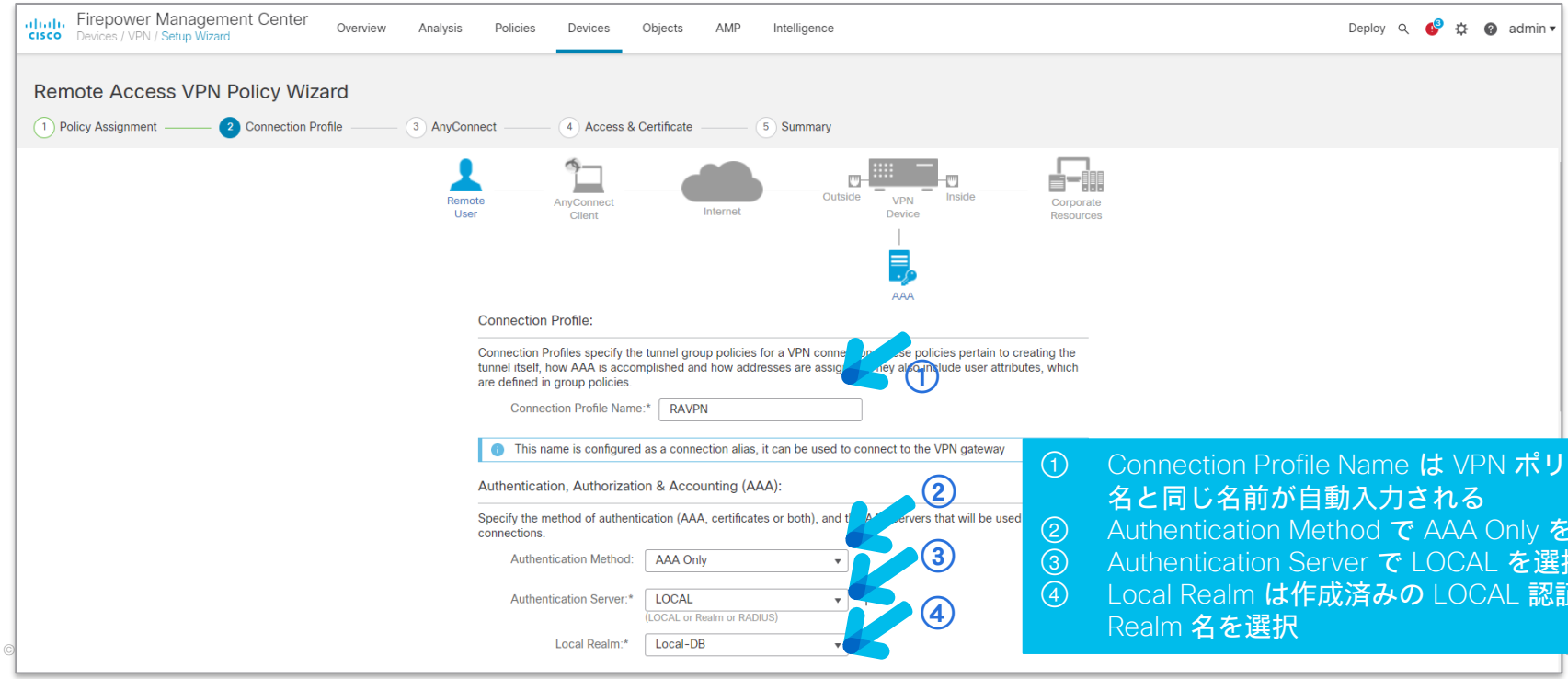
Wizard を使用した RAVPN ポリシー設定

- リモートアクセス VPN のポリシーを設定
  Devices > VPN > Remote Access
- VPN プロトコルの選択、および VPN 終端デバイスの選択



Wizard を使用した RAVPN ポリシー設定

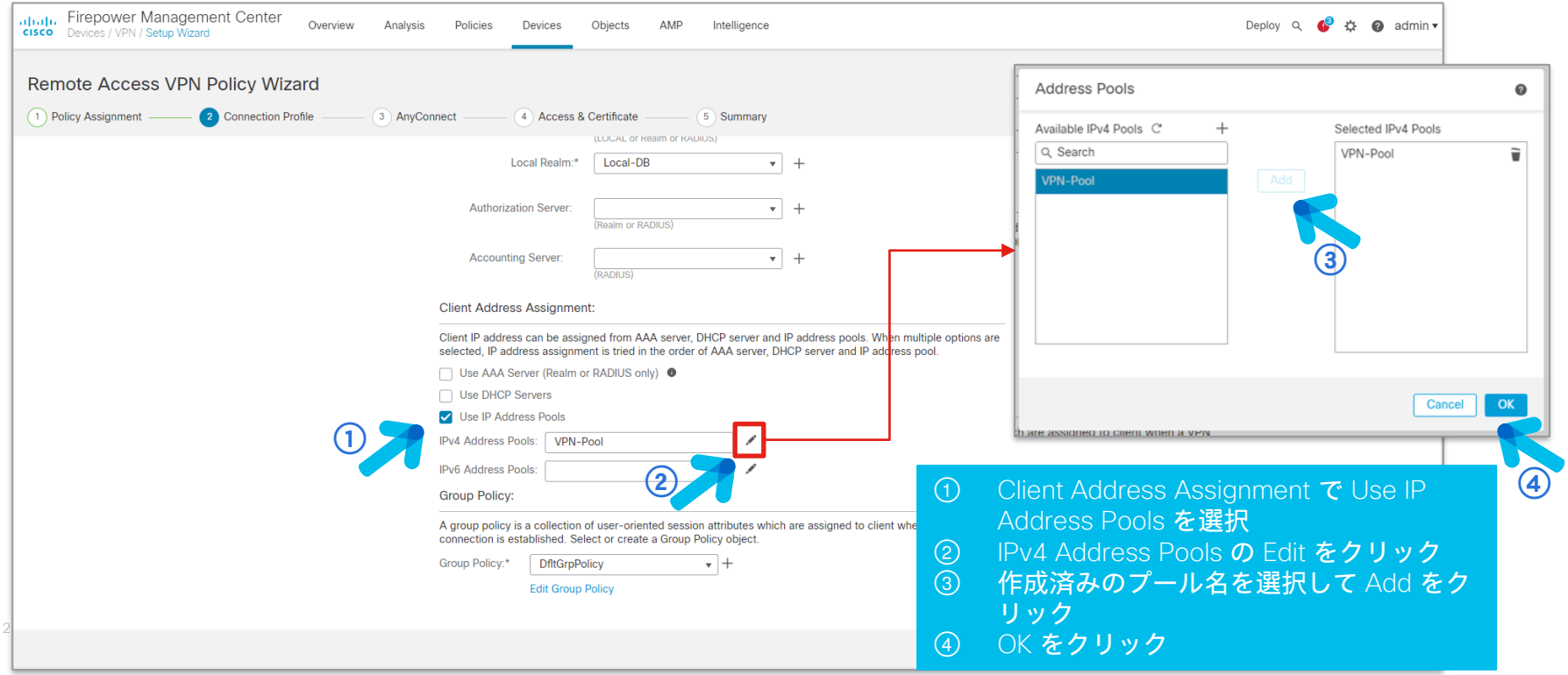
- 認証方式の選択



① Connection Profile Name は VPN ポリシー名と同じ名前が自動入力される
② Authentication Method で AAA Only を選択
③ Authentication Server で LOCAL を選択
④ Local Realm は作成済みの LOCAL 認証用 Realm 名を選択

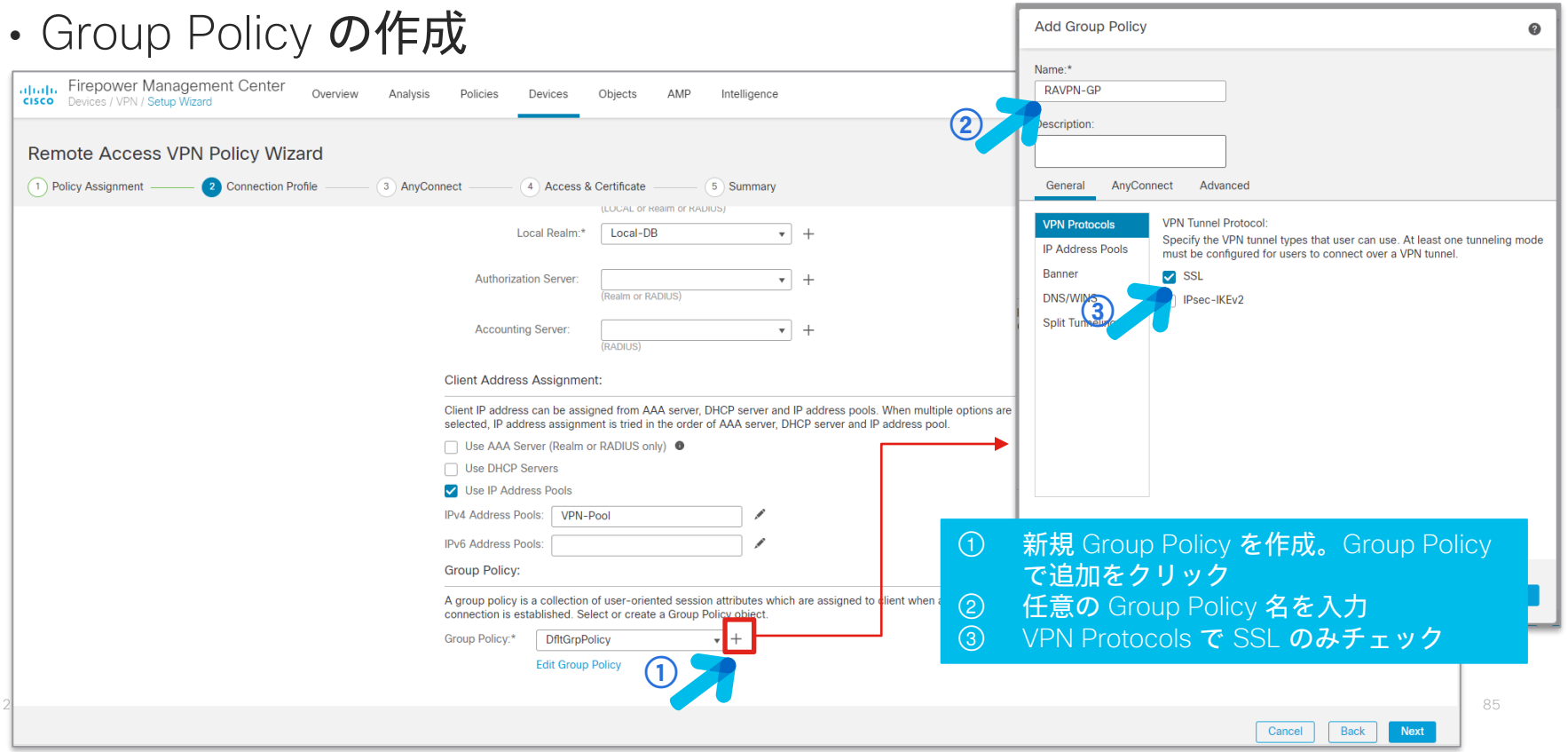
Wizard を使用した RAVPN ポリシー設定

- VPN プールアドレスの指定



Wizard を使用した RAVPN ポリシー設定

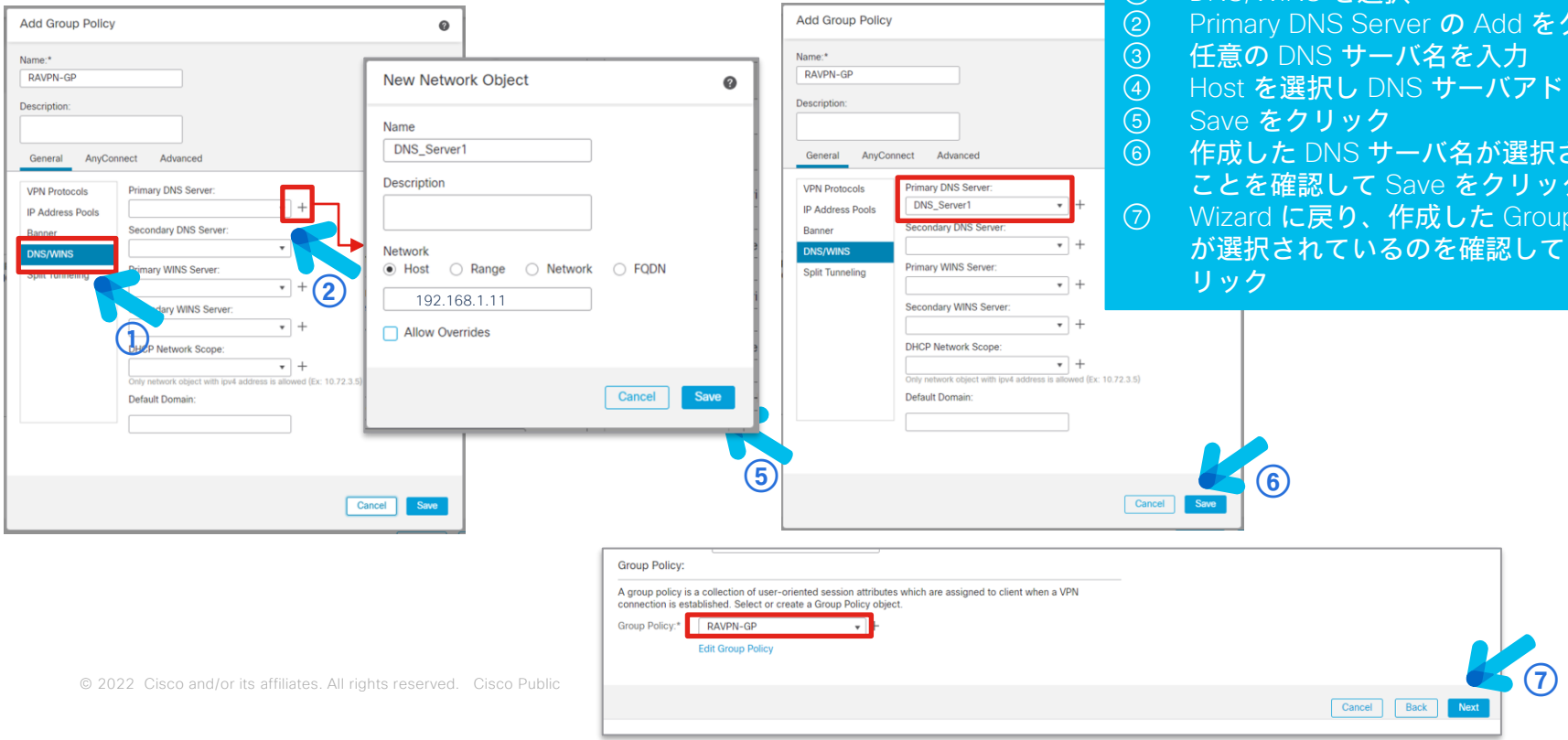
- Group Policy の作成



Wizard を使用した RAVPN ポリシー設定

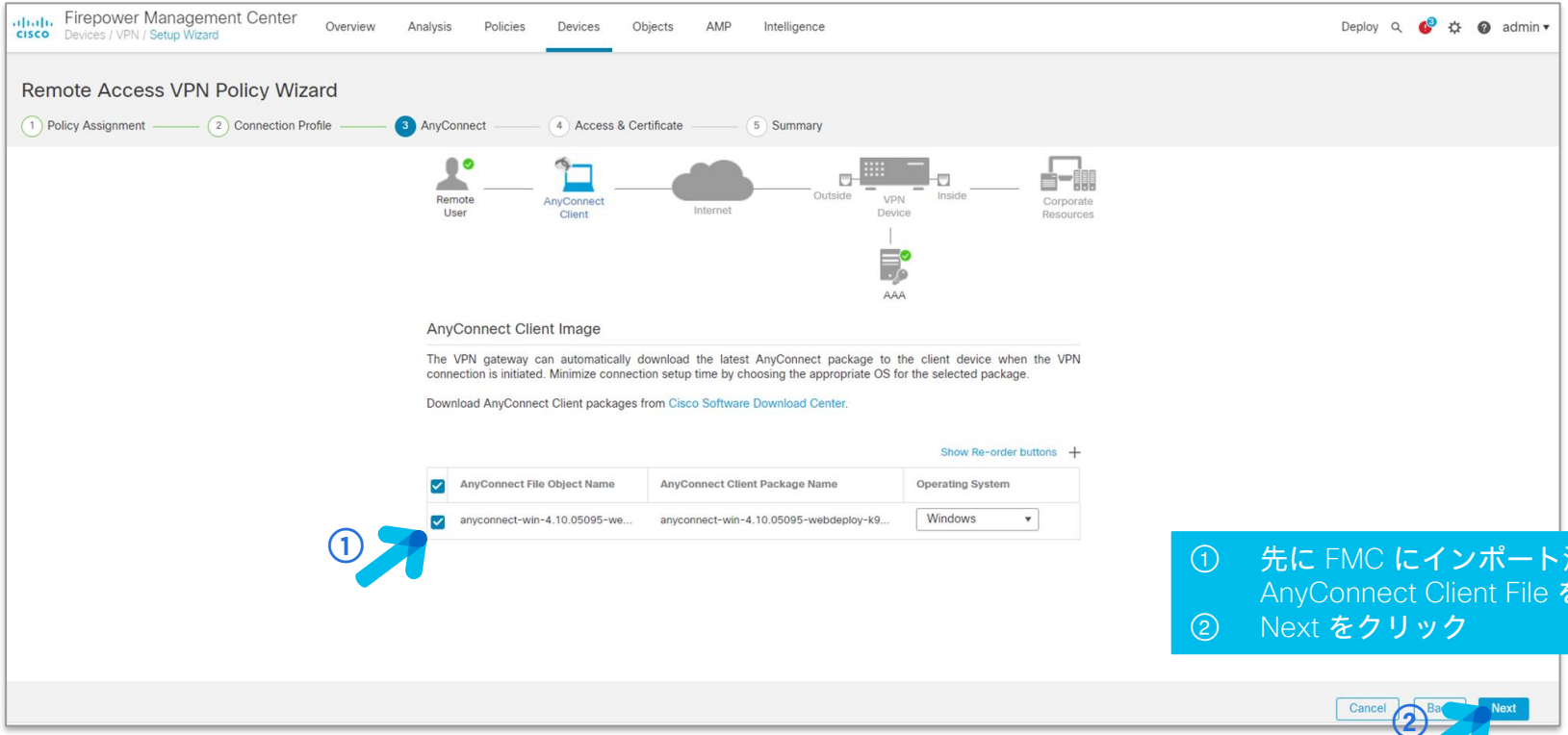
- Group Policy での DNS サーバ設定

前ページの続き
① DNS/WINS を選択
② Primary DNS Server の Add をクリック
③ 任意の DNS サーバ名を入力
④ Host を選択し DNS サーバアドレスを入力
⑤ Save をクリック
⑥ 作成した DNS サーバ名が選択されていることを確認して Save をクリック
⑦ Wizard に戻り、作成した Group Policy 名が選択されているのを確認して Next をクリック



Wizard を使用した RAVPN ポリシー設定

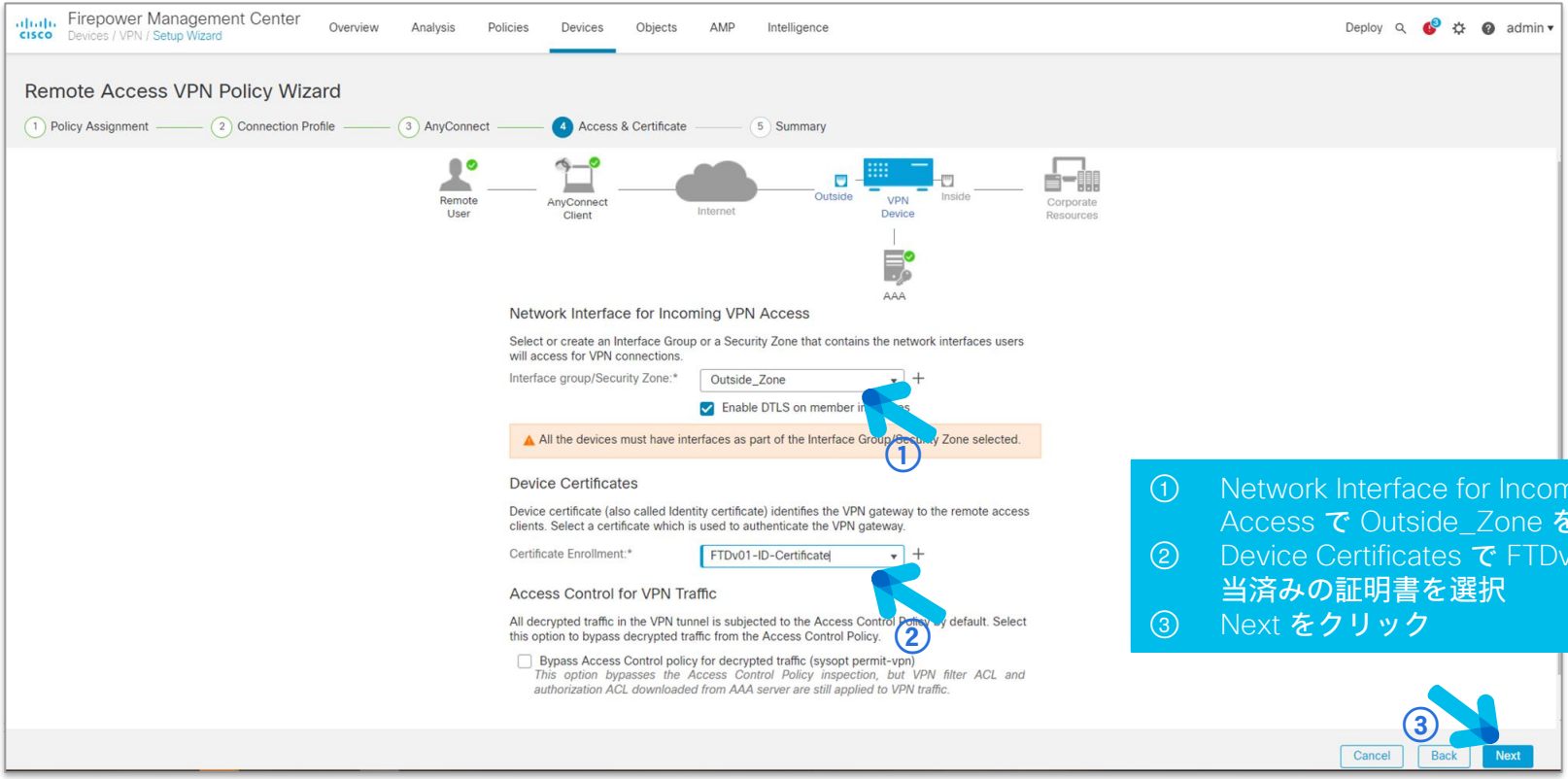
- AnyConnect Client Image の指定



① 先に FMC にインポート済の AnyConnect Client File を選択
② Next をクリック

Wizard を使用した RAVPN ポリシー設定

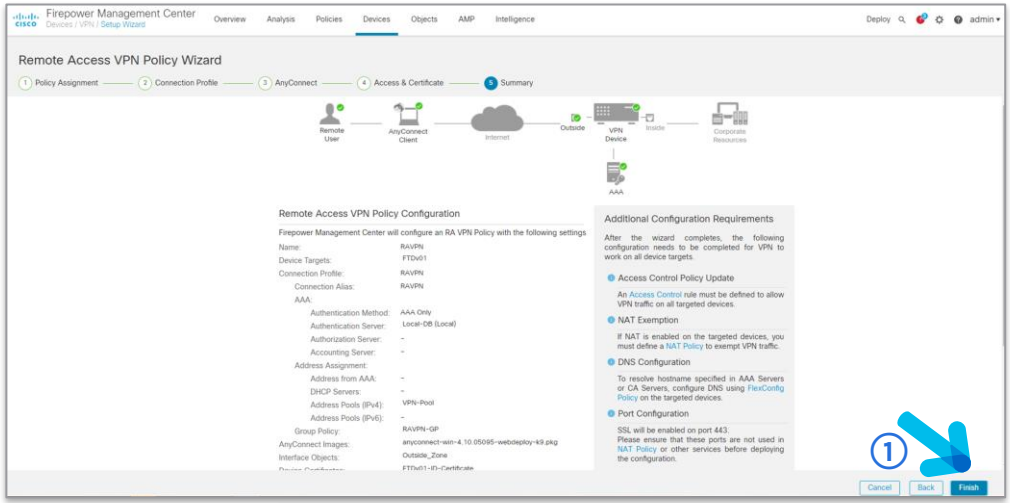
- VPN アクセスインタフェースの指定、および ID 証明書の指定



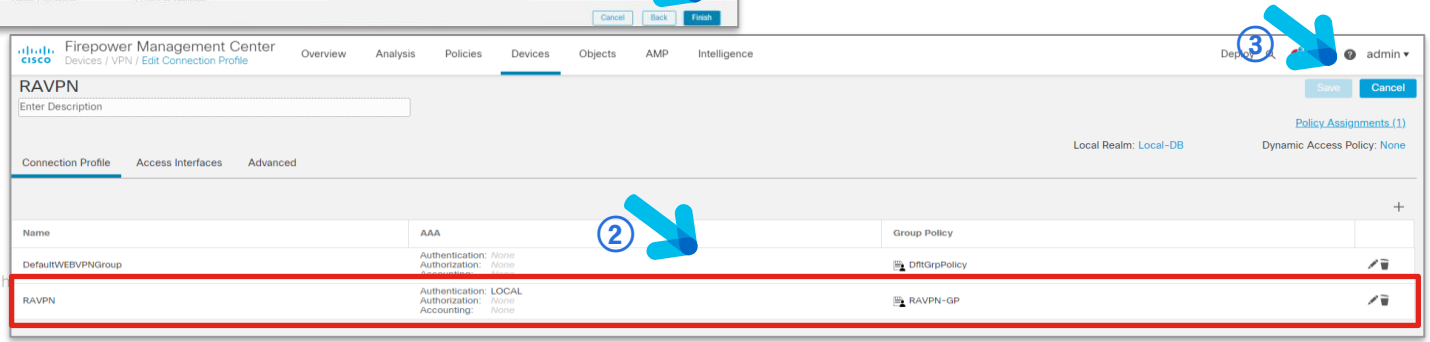
① Network Interface for Incoming VPN Access で Outside_Zone を選択
② Device Certificates で FTDv01 に割当済みの証明書を選択
③ Next をクリック

Wizard を使用した RAVPN ポリシー設定

- Wizard 設定内容の確認



① Wizard で設定された内容を確認し、問題なければ Finish をクリック
② 新しい接続プロファイルが作成されていることを確認
③ SAVE をクリック

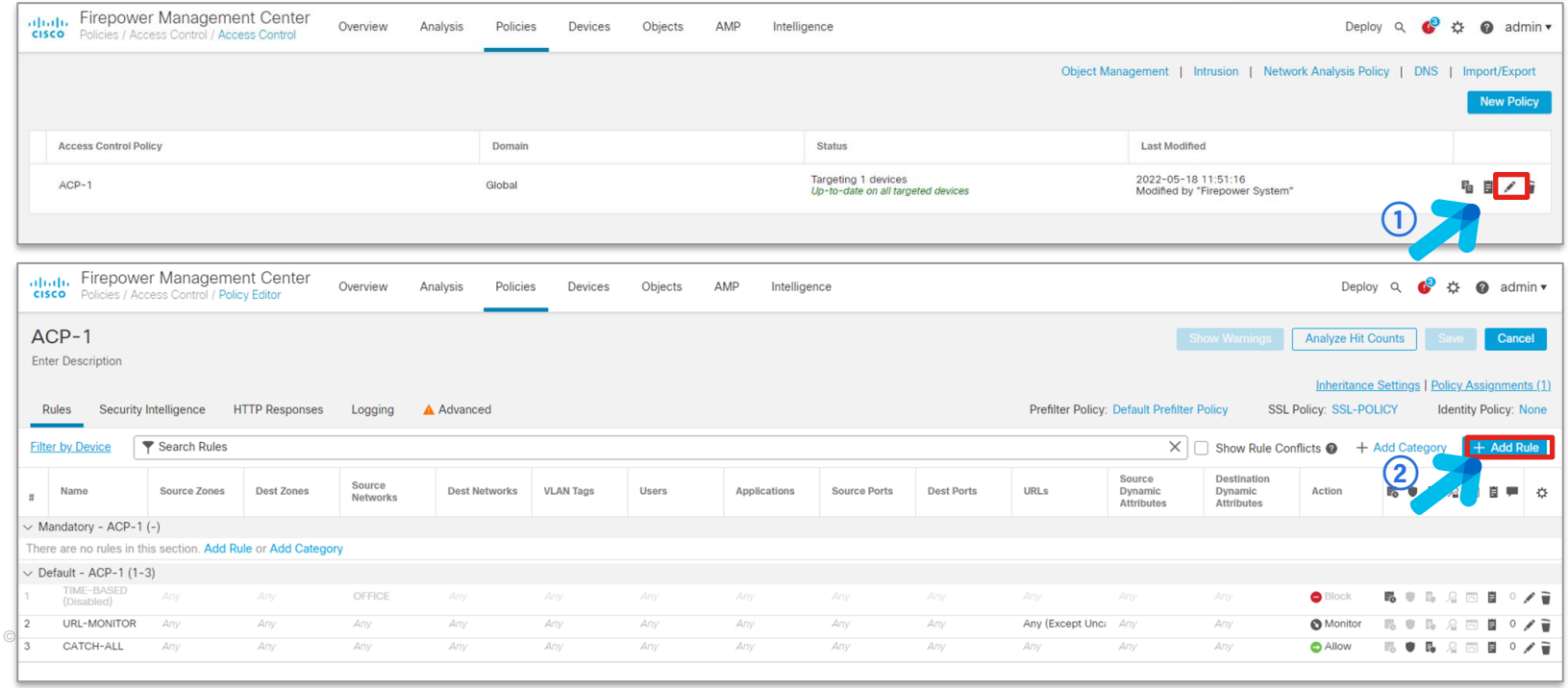


リモートアクセス用 ACP ルール設定

- RAVPN アクセス時にも Intrusion & File ポリシーを適用する ACP ルールを追加

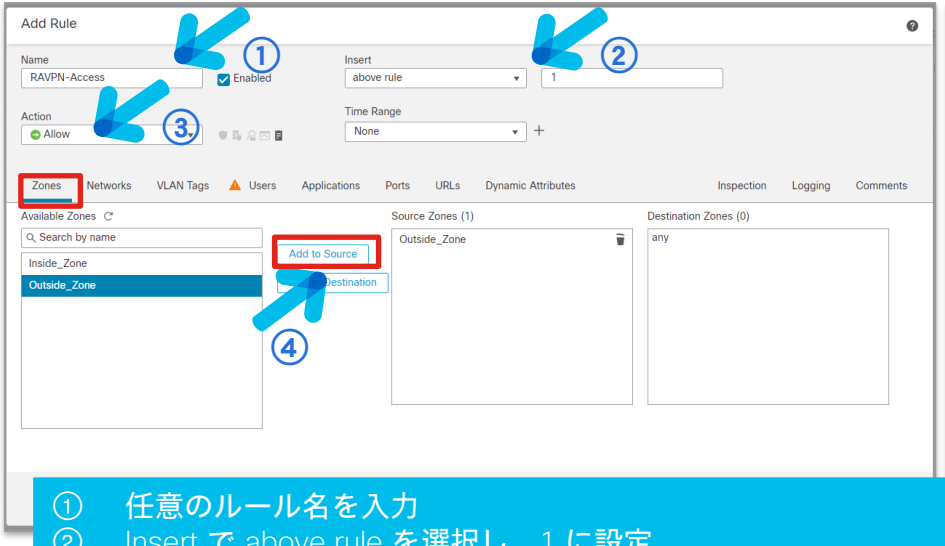
Policies > Access Control > Access Control

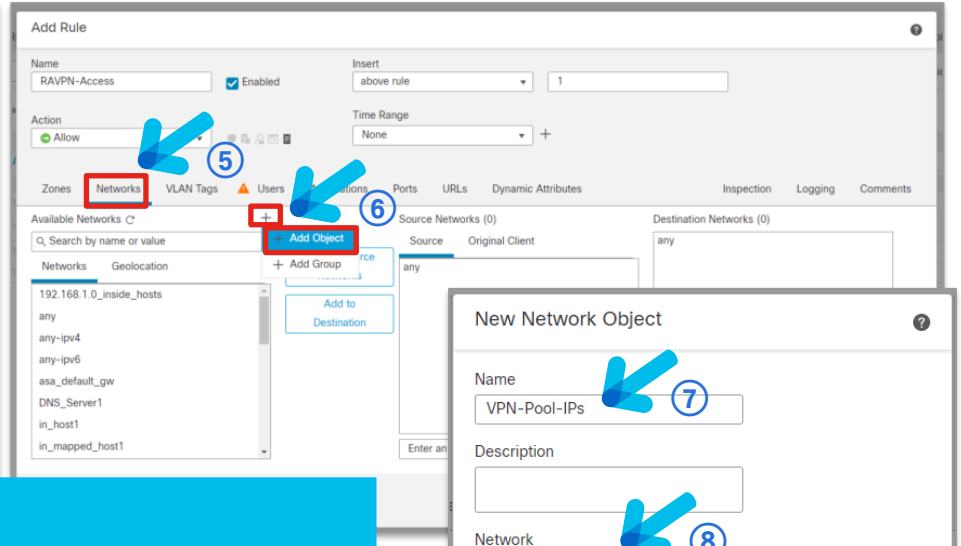
① ACP-1 の Edit をクリック
② Add Rule をクリック

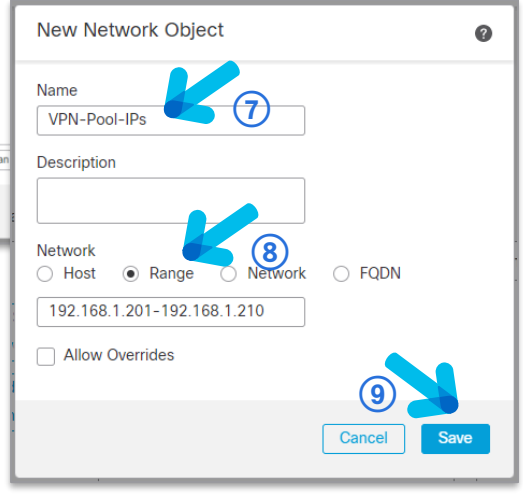


リモートアクセス用 ACP ルール設定

- Zones, Networks (VPN プールアドレスの Network Object 作成)



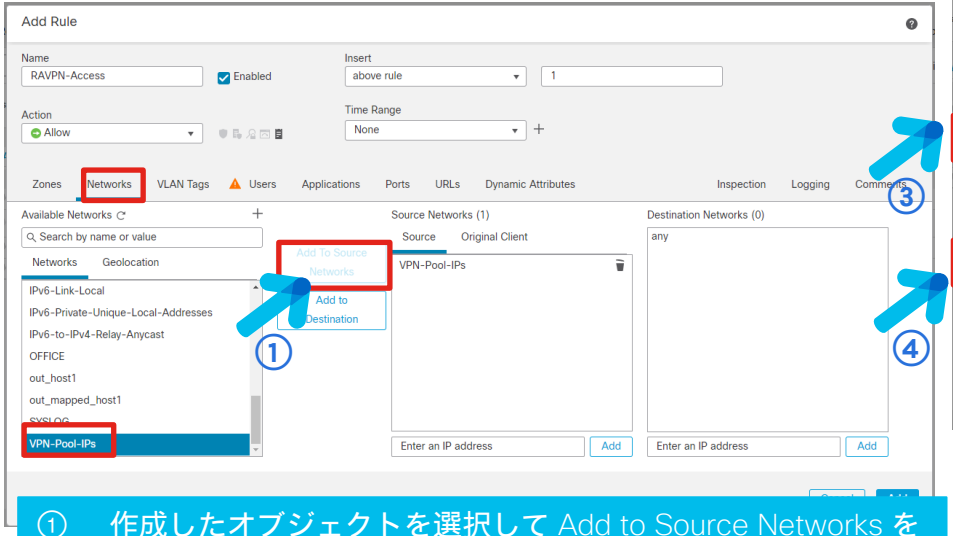


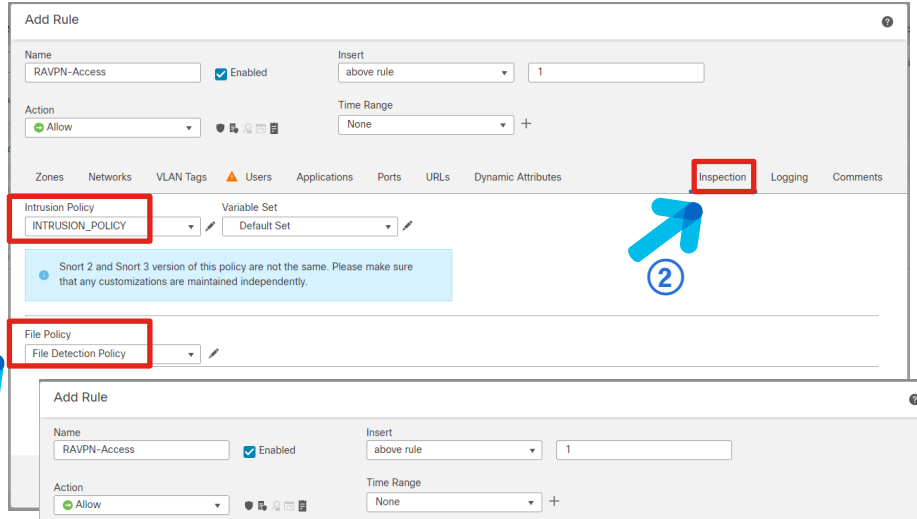


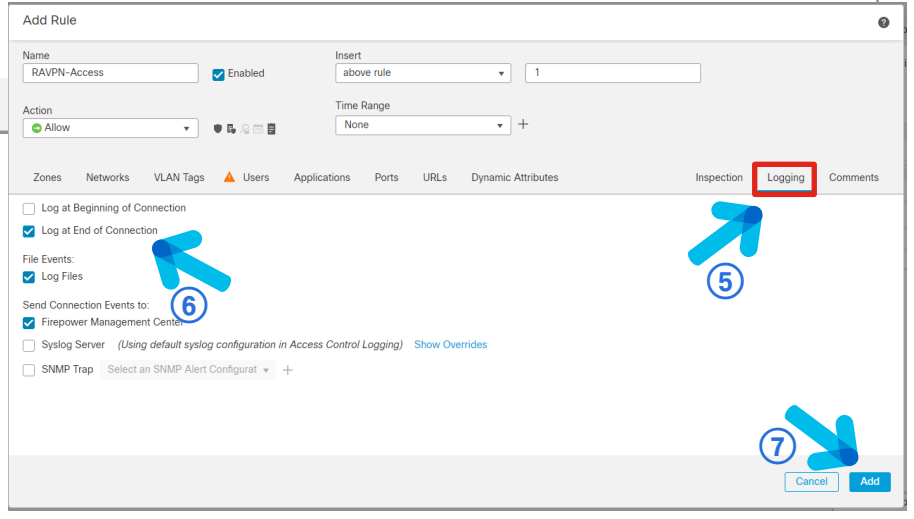
① 任意のルール名を入力
② Insert で above rule を選択し、1 に設定
③ Action は Allow を選択
④ Zones タブで Available Zones から Outside_Zone を選択し、Add to Source をクリック
⑤ Networks タブを選択
⑥ Available Networks の追加を選択し、Add Object を選択
⑦ New Network Object で VPN プールオブジェクトを作成。任意の名前を入力
⑧ Network で Range を指定し、設定した VPN プールと同じアドレス範囲を入力

リモートアクセス用 ACP ルール設定

- Networks, Inspection, Logging



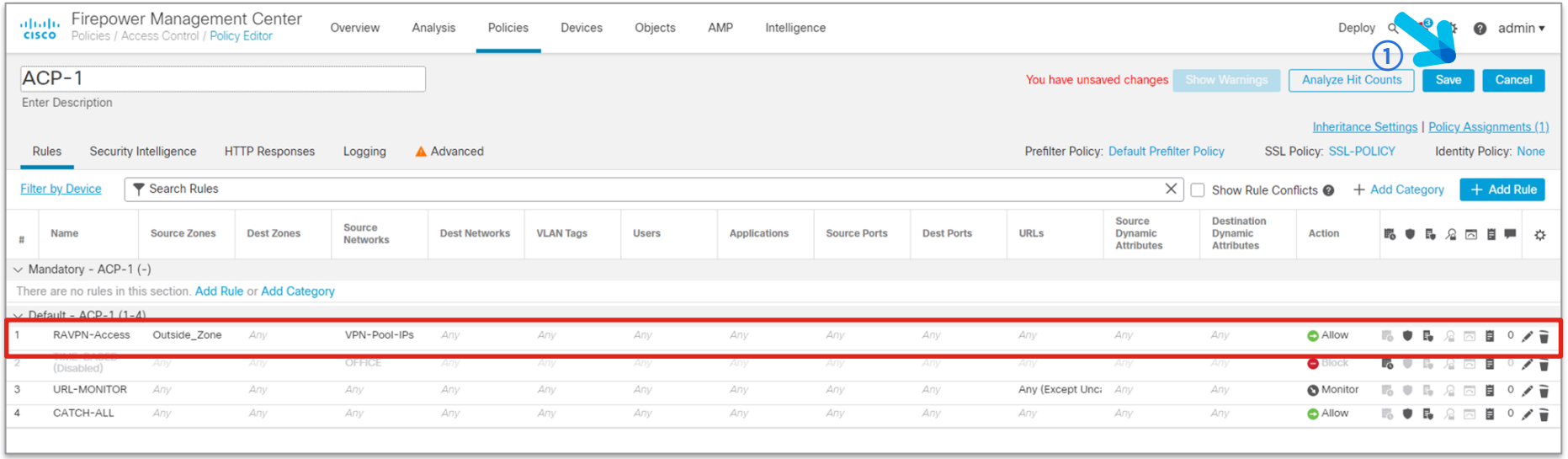




① 作成したオブジェクトを選択して Add to Source Networks をクリック
② Inspection タブをクリック
③ Intrusion Policy で作成済の INTRUSION_POLICY を選択
④ File Policy で作成済の File Detection Policy を選択
⑤ Logging タブを選択
⑥ Log at End of Connection を選択
⑦ Add をクリック

リモートアクセス用 ACP ルール設定

- ACP ルールの保存



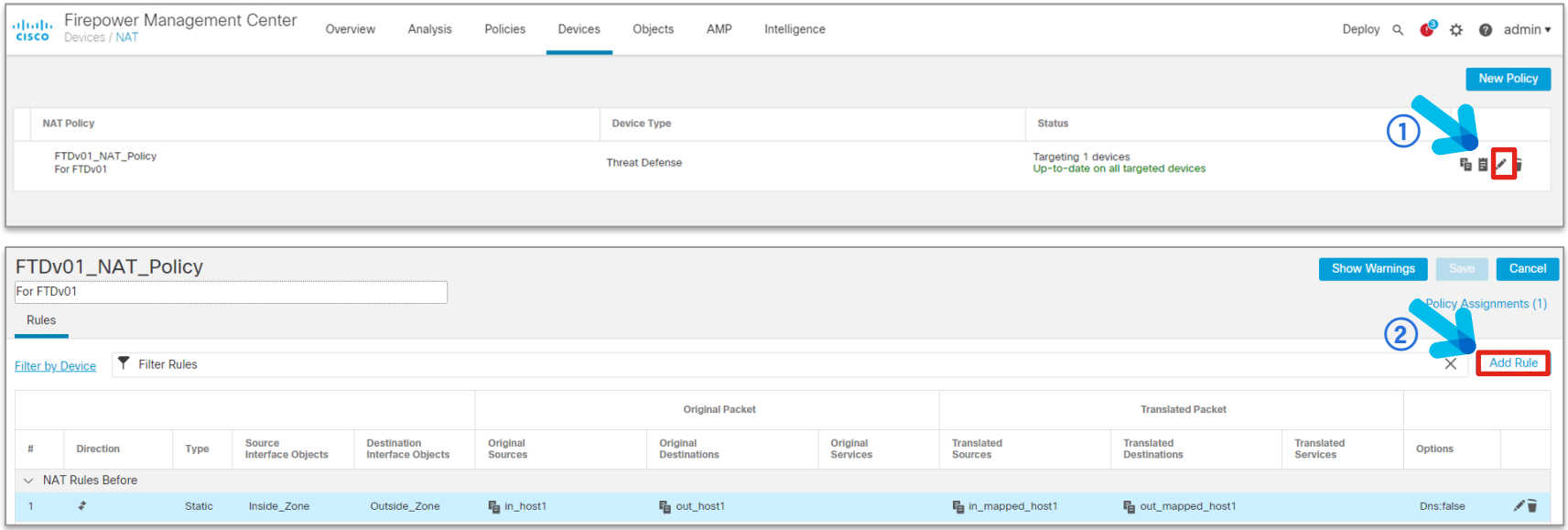
① Save をクリックして設定を保存

リモートアクセス用の NAT 除外設定

- RAVPN 接続クライアントからの通信が FTD に戻るときに NAT されないように、RAVPN 通信用の NAT 除外ルールを追加

① 既存の NAT ポリシーの Edit をクリック
② Add Rule をクリック

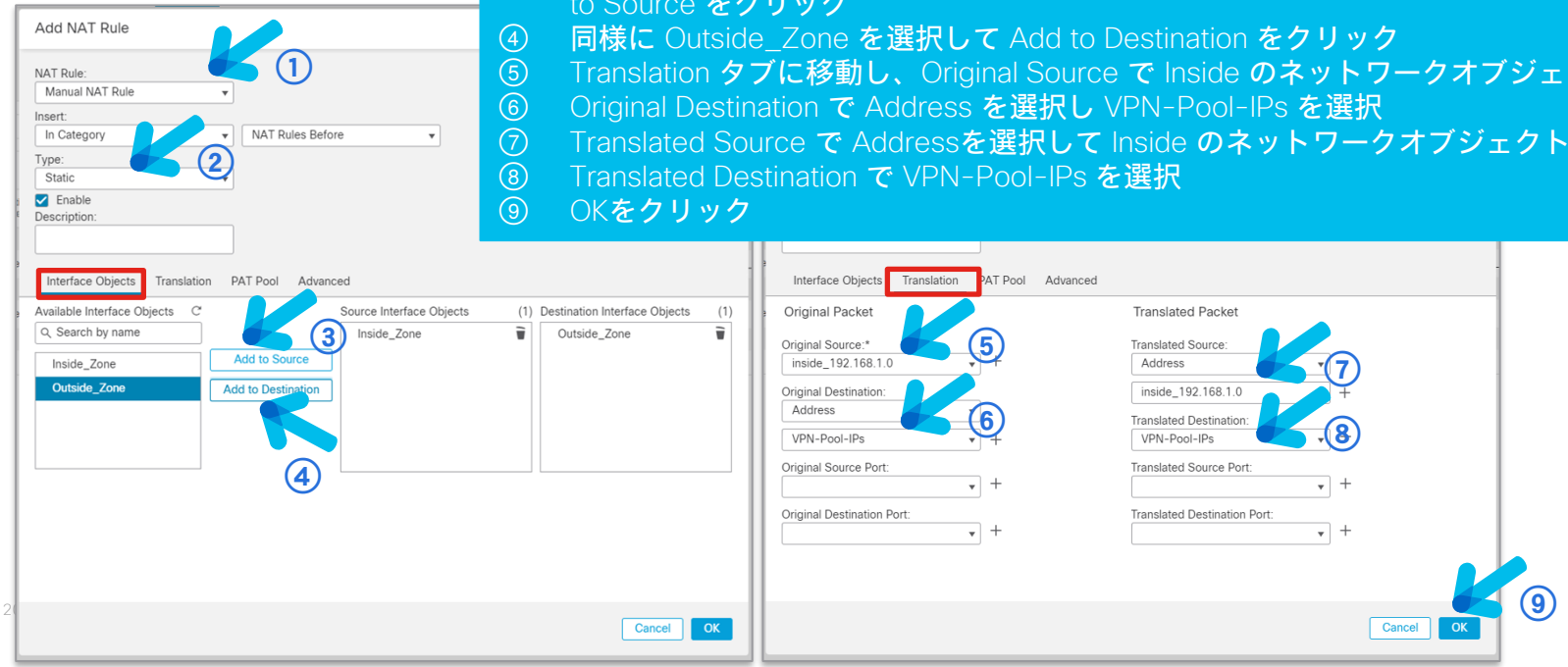
Devices > NAT



リモートアクセス用の NAT 除外設定

- Interface Objects, Translation

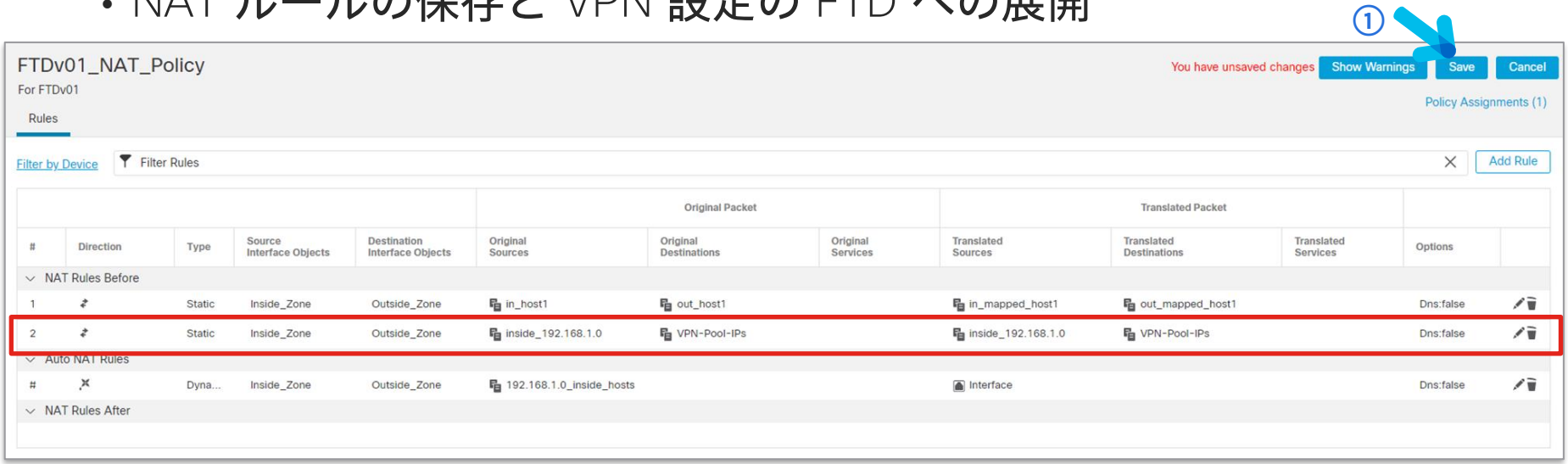
① Manual NAT Rule を選択
② Type で Static を選択
③ Interface Objects タブで、Available Interface Objects から Inside_Zone を選択して Add to Source をクリック
④ 同様に Outside_Zone を選択して Add to Destination をクリック
⑤ Translation タブに移動し、Original Source で Inside のネットワークオブジェクトを選択
⑥ Original Destination で Address を選択し VPN-Pool-IPs を選択
⑦ Translated Source で Addressを選択して Inside のネットワークオブジェクトを選択
⑧ Translated Destination で VPN-Pool-IPs を選択
⑨ OKをクリック

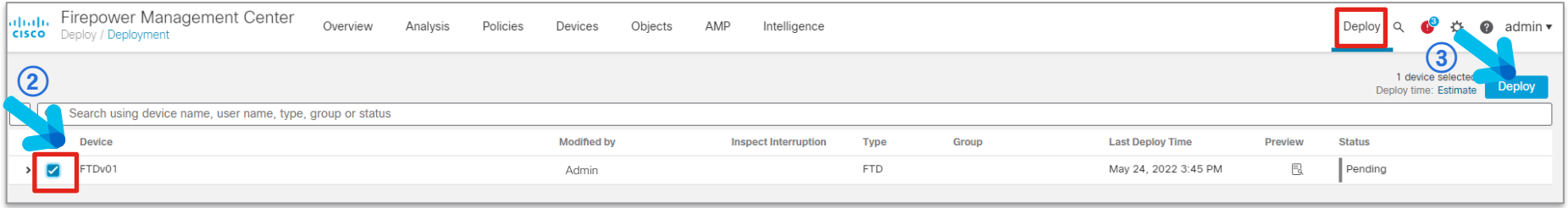


リモートアクセス用の NAT 除外設定

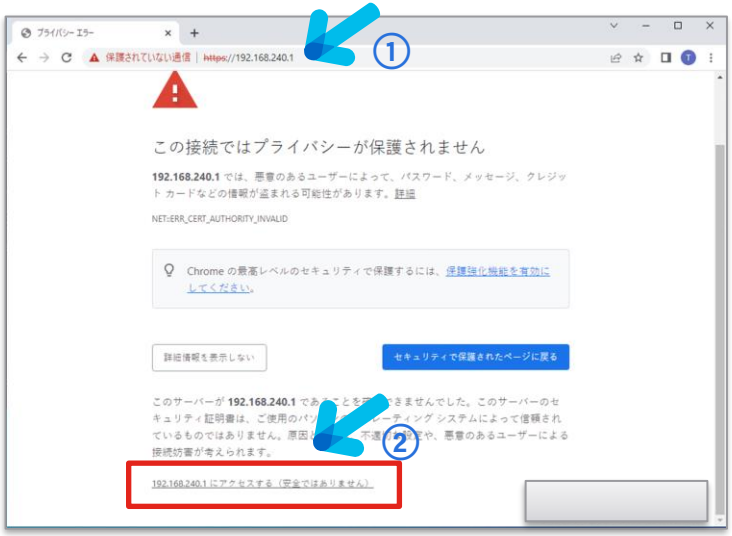
- NAT ルールの保存と VPN 設定の FTD への展開

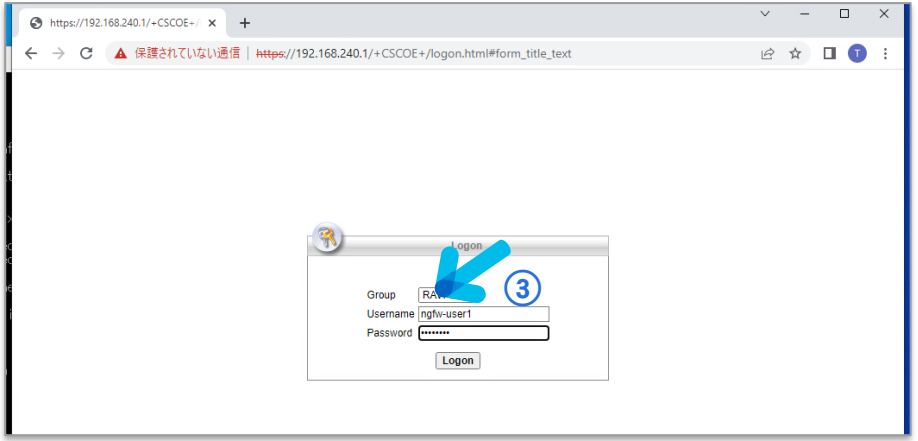
① 右上の Save ボタンをクリックして設定を保存
② Deploy を選択し、FTDv01 を選択
③ Deploy ボタンをクリック

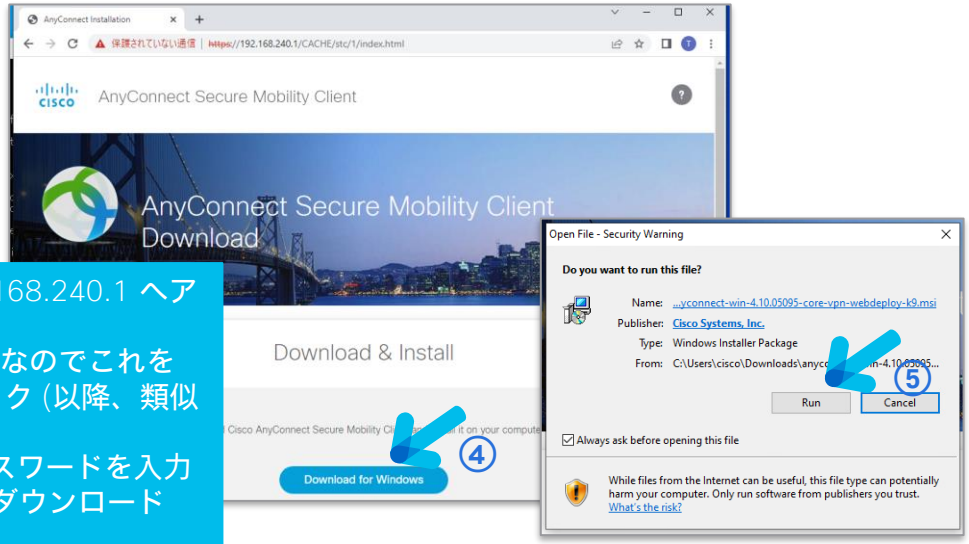




接続テスト

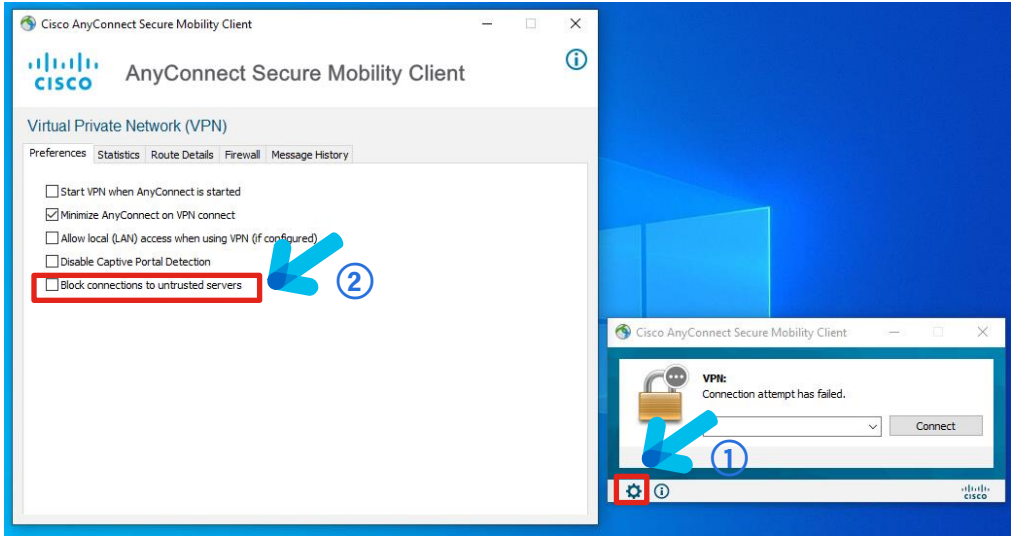


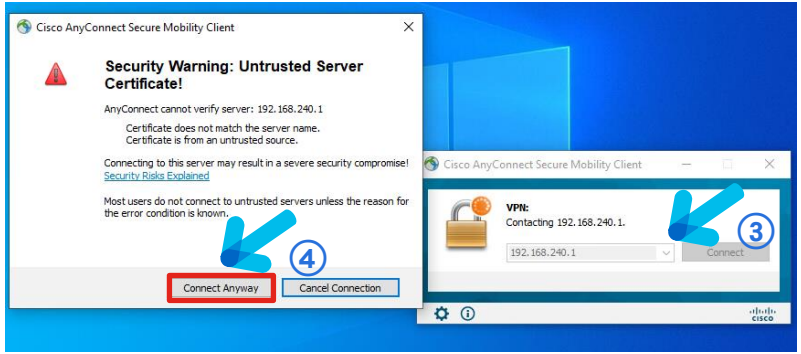


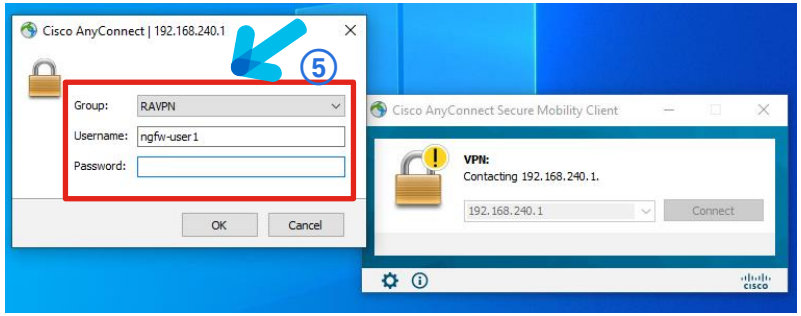


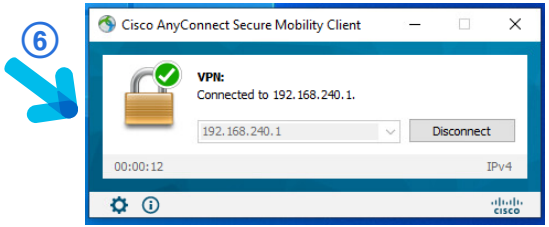
① 今回はテスト接続のため test PC-2 のブラウザで https://192.168.240.1 へアクセス
② プライバシー接続のエラーが表示されるが、今回はテスト接続なのでこれを無視し、そのまま「192.168.240.1 にアクセスする」をクリック（以降、類似エラーは無視することとする）
③ Group で RAVPN を選択し、Local DB で設定したユーザ名/パスワードを入力
④ Download for Windows をクリックして AnyConnect Client をダウンロード
⑤ test PC-2 にて AnyConnect Client をインストール

接続テスト





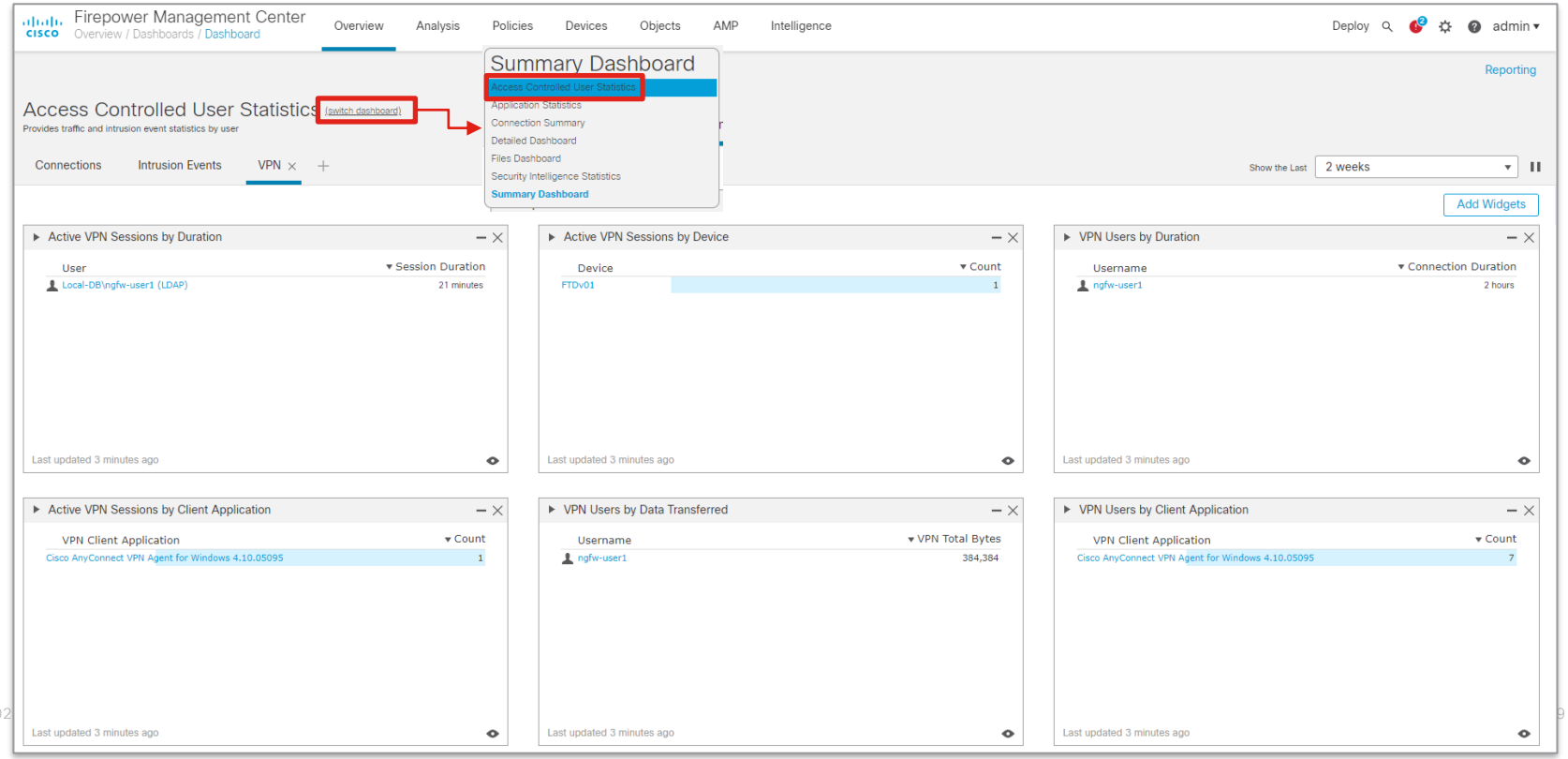




① AnyConnect Client を起動しギアマークをクリック
② Preferences で Block connections to untrusted servers のチェックを外す
③ AnyConnect Client で 192.168.240.1 を入力して Connect をクリック
④ Security Warning が表示されるが Connect Anyway をクリック
⑤ ユーザ名/パスワードを入力して OK をクリック
⑥ RAVPN 接続完了

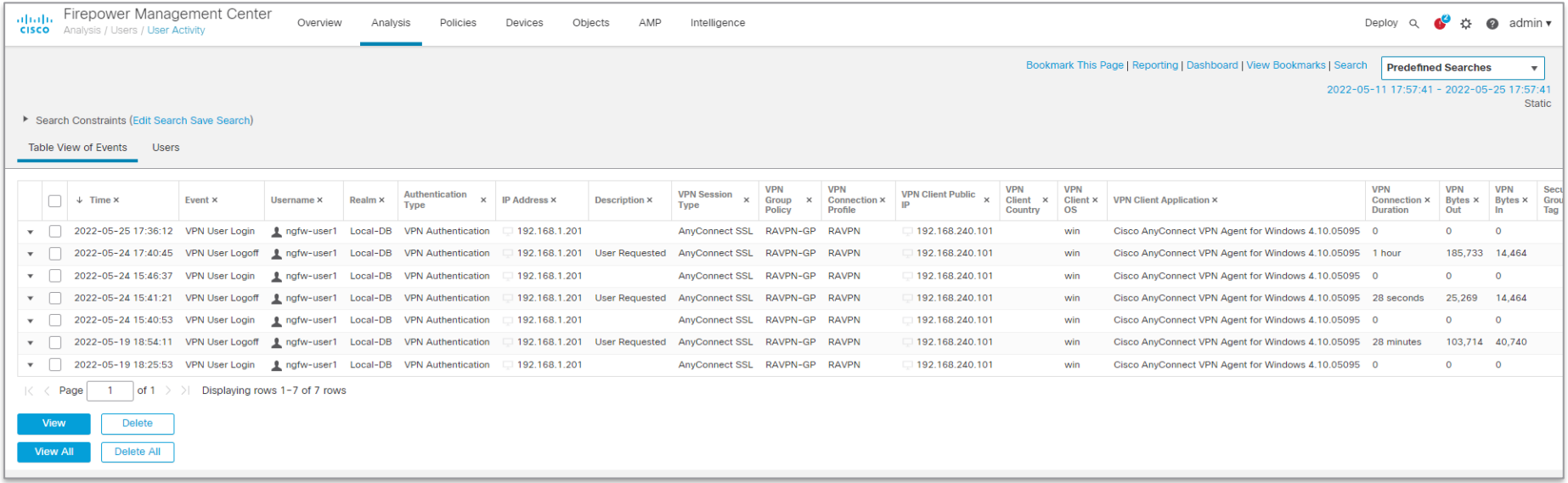
Monitoring Events

- Overview > switch dashboard > Access Controlled User Statistics



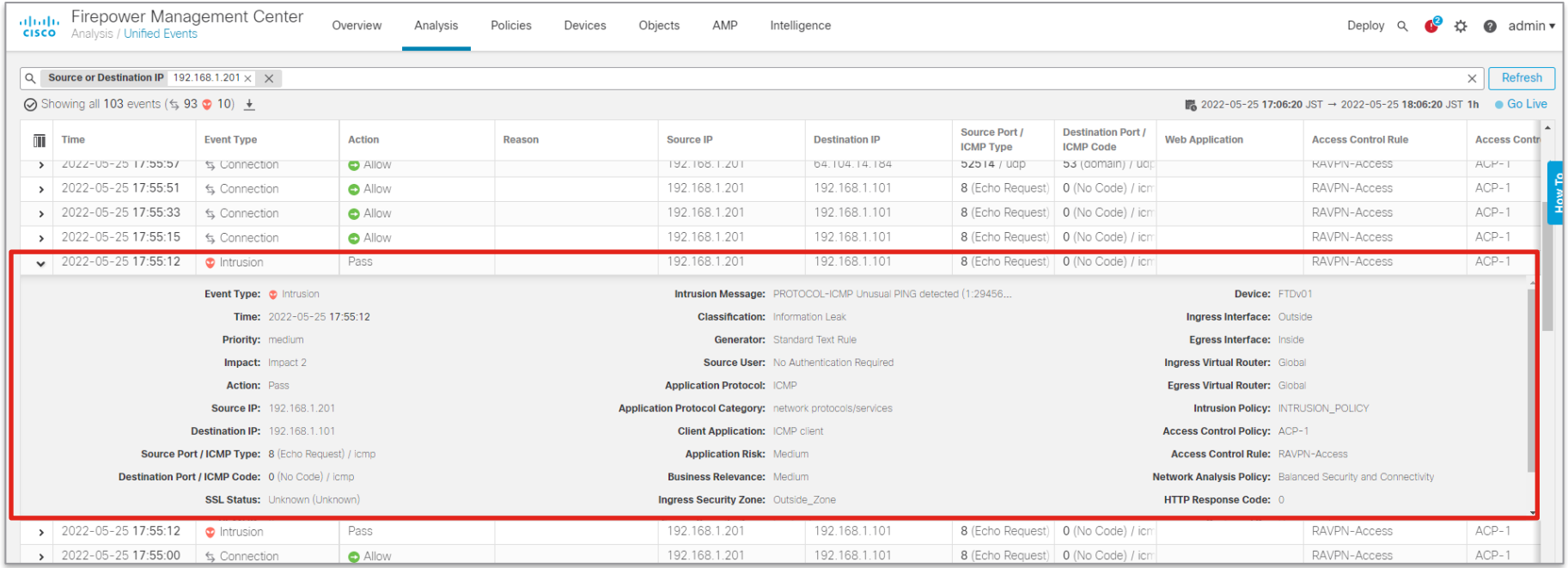
Monitoring Events

- Analysis > Users > User Activity



Monitoring Events

- Unified Events
  - VPN 端末 192.168.1.201 から 内部端末 192.168.1.101 への ICMP 通信を Intrusion Policy で検知



CLI での確認

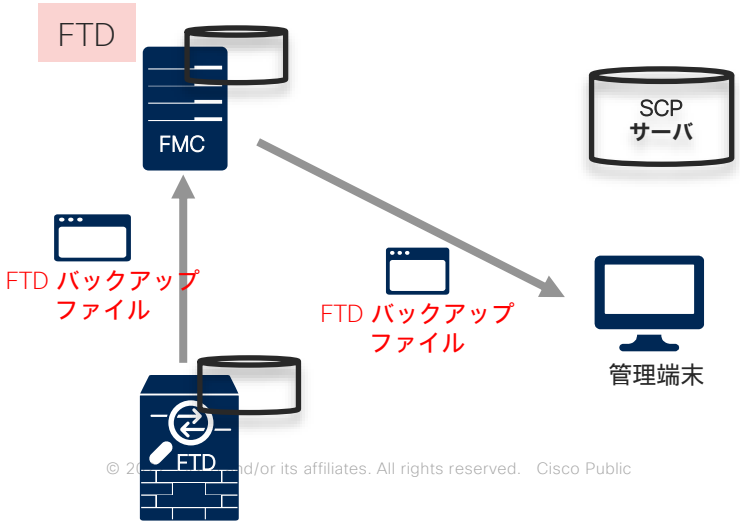
- FTDv01 上での show command – show vpn-sessiondb anyconnect

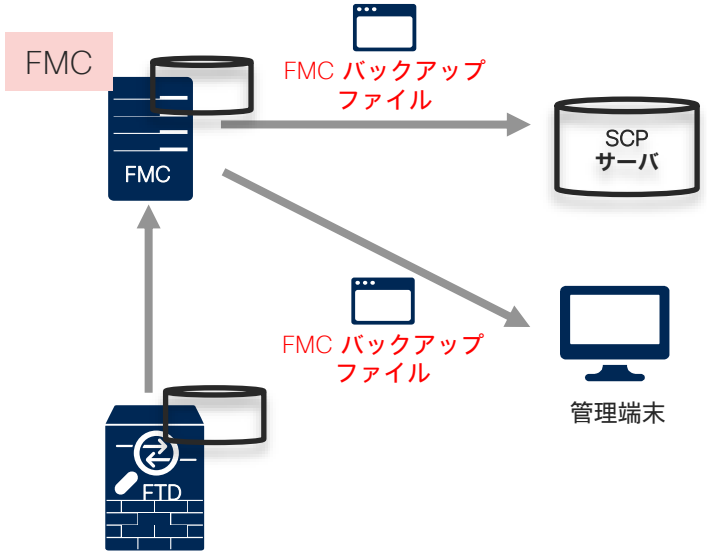
```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : ngfw-user1            Index        : 7
Assigned IP  : 192.168.1.201         Public IP    : 192.168.240.101
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 14464                 Bytes Rx     : 29650
Group Policy : RAVPN-GP              Tunnel Group : RAVPN
Login Time   : 08:36:12 UTC Wed May 25 2022
Duration     : 0h:11m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a8f00100007000628dea7c
Security Grp : none                  Tunnel Zone  : 0
```

14. バックアップの設定とリストアの方法

バックアップについて

- FMC, FTD ともにバックアップの取得が可能
- FTD バックアップの保存先は FTD ローカル、もしくは FMC ローカル
- FMC バックアップは FMC ローカルへのダウンロード、およびリモートサーバ (SCP) へコピー
- FMC に保存したバックアップファイルは、FMC の GUI より管理端末へダウンロードすることが可能





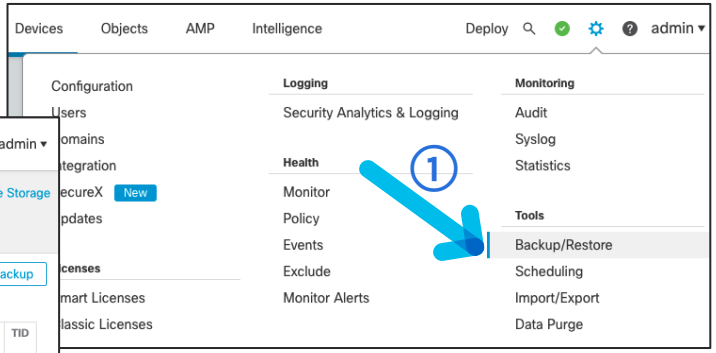
本章のバックアップに関する操作の流れ

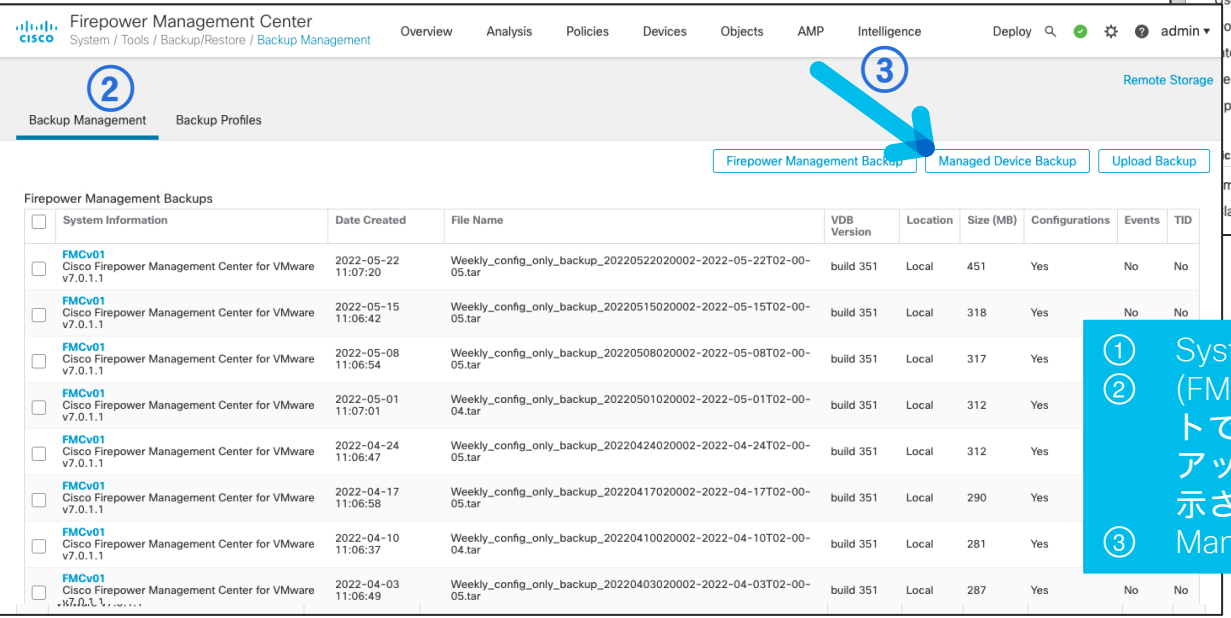
- FTD デバイスのバックアップ取得
- FTD デバイスのバックアップファイル確認
- FMC のバックアップ取得
- FMC のバックアップファイル確認

  - SCP サーバは、管理ネットワークに存在している PC を利用
  - FTD, FMC ともに HA でもバックアップ取得は可能

FTD デバイスのバックアップ取得 ①

- FMC で管理している FTD デバイスのバックアップを取得

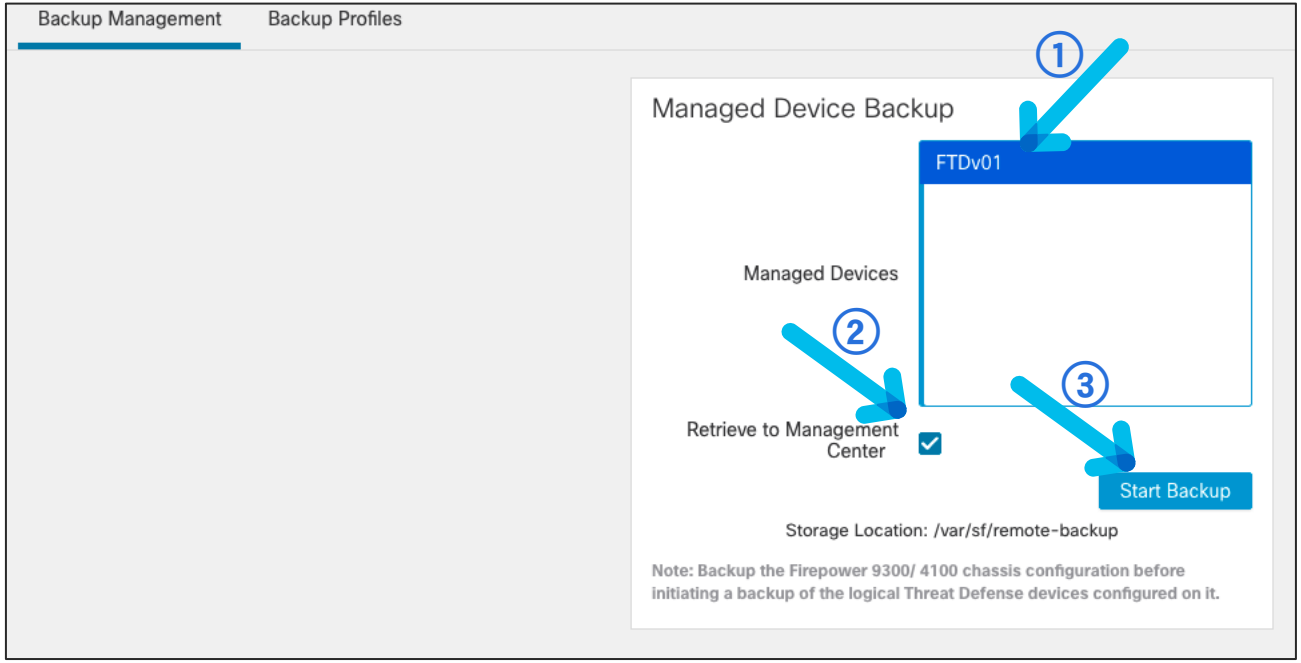




① System (歯車マーク) → Backup/Restore を選択
② (FMC を新規でインストールした場合) デフォルトでスケジューリングされた FMC のバックアップデータが存在していれば、その一覧が表示されている
③ Managed Device Backup をクリック

FTD デバイスのバックアップ取得 ②

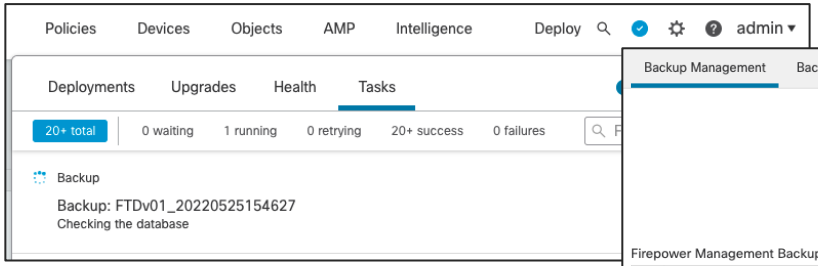
- バックアップの取得対象とする FTD デバイスを指定

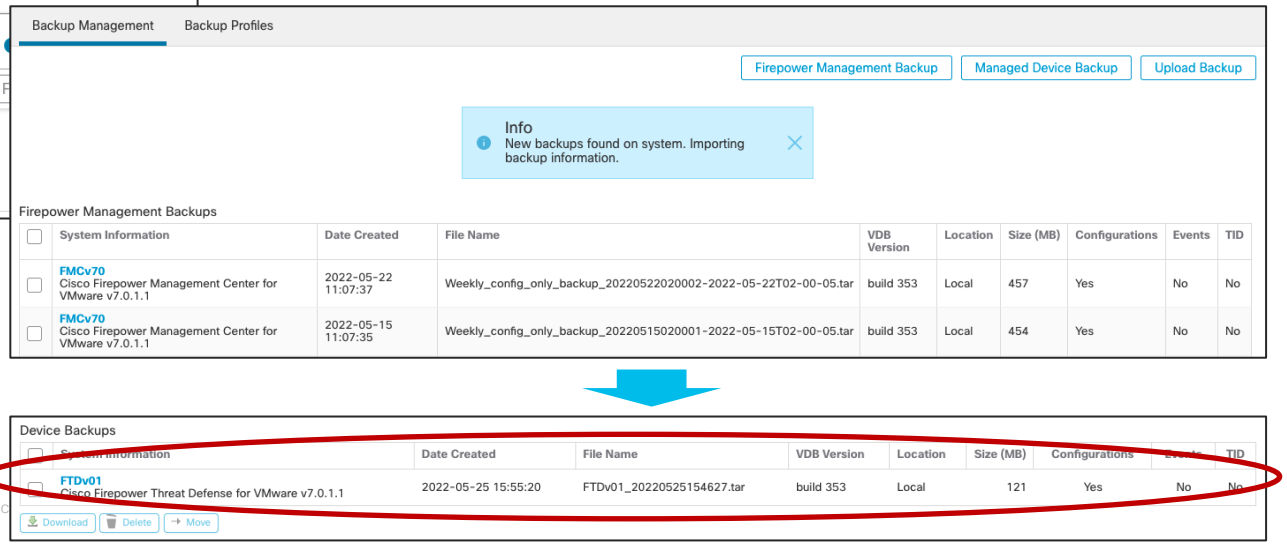


① バックアップ取得対象の FTD デバイスを選択
② 取得したバックアップファイルを FMC へ移動する場合、Retrieve to Management Center にチェックを入れる。チェックを入れなければバックアップファイルは FTD デバイスの /var/sf/backup に保存される
③ Start Backup をクリック

FTD デバイスのバックアップ確認

- バックアップ処理がスタートしたことを Task Tab (system の左隣) で確認
- 完了後に Backup Management のページをスクロールダウン、Device Backups に取得したバックアップファイルの存在を確認

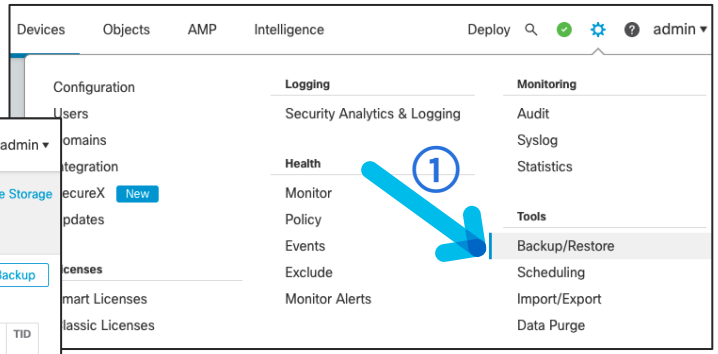


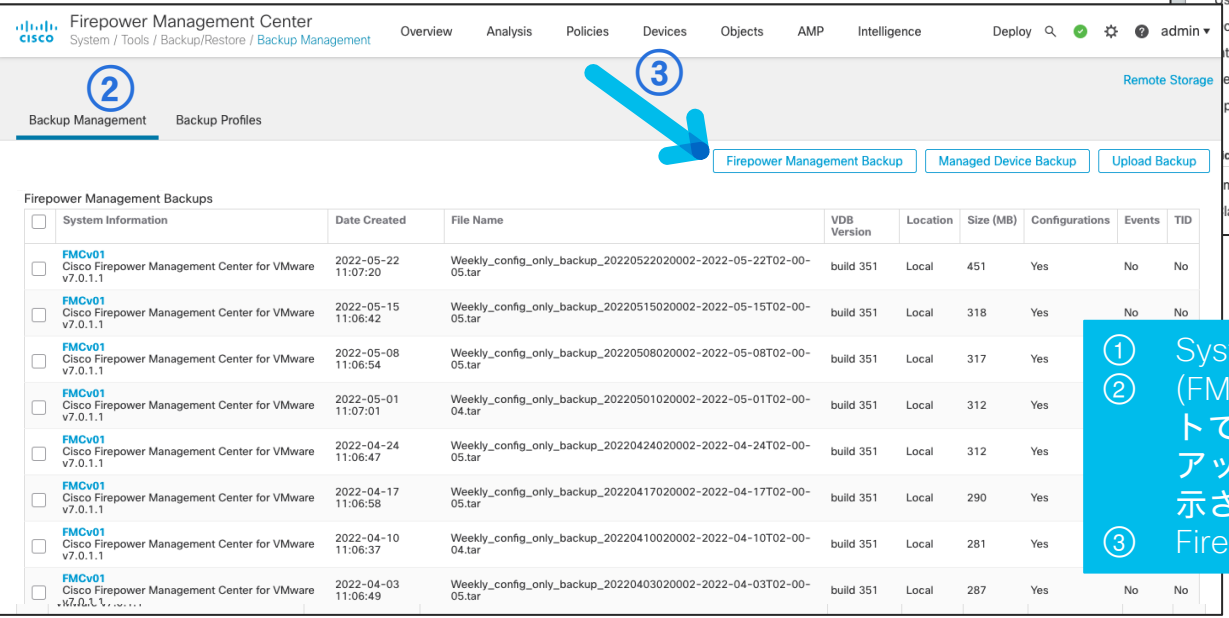


- バックアップファイルは、管理用 PC ローカルにダウンロードして保存しておく (リストアで利用)

FMC のバックアップ取得 ①

- FMC 自身のバックアップを取得

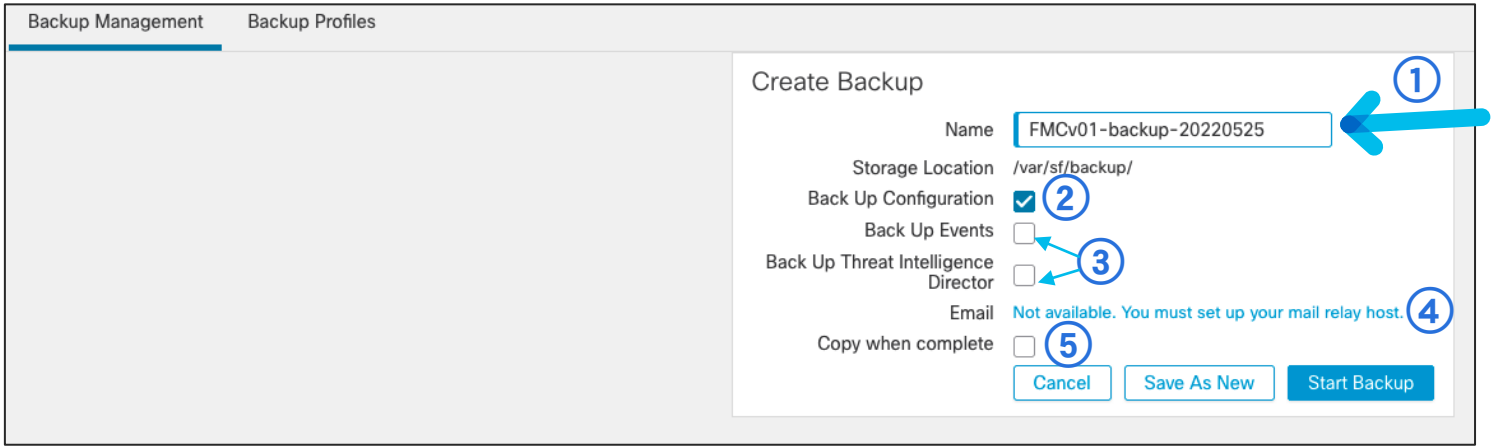




① System (歯車マーク) → Backup/Restore を選択
② (FMC を新規でインストールした場合) デフォルトでスケジューリングされた FMC のバックアップデータが存在していれば、その一覧が表示されている
③ Firepower Management Backup をクリック

FMC のバックアップ取得 ②

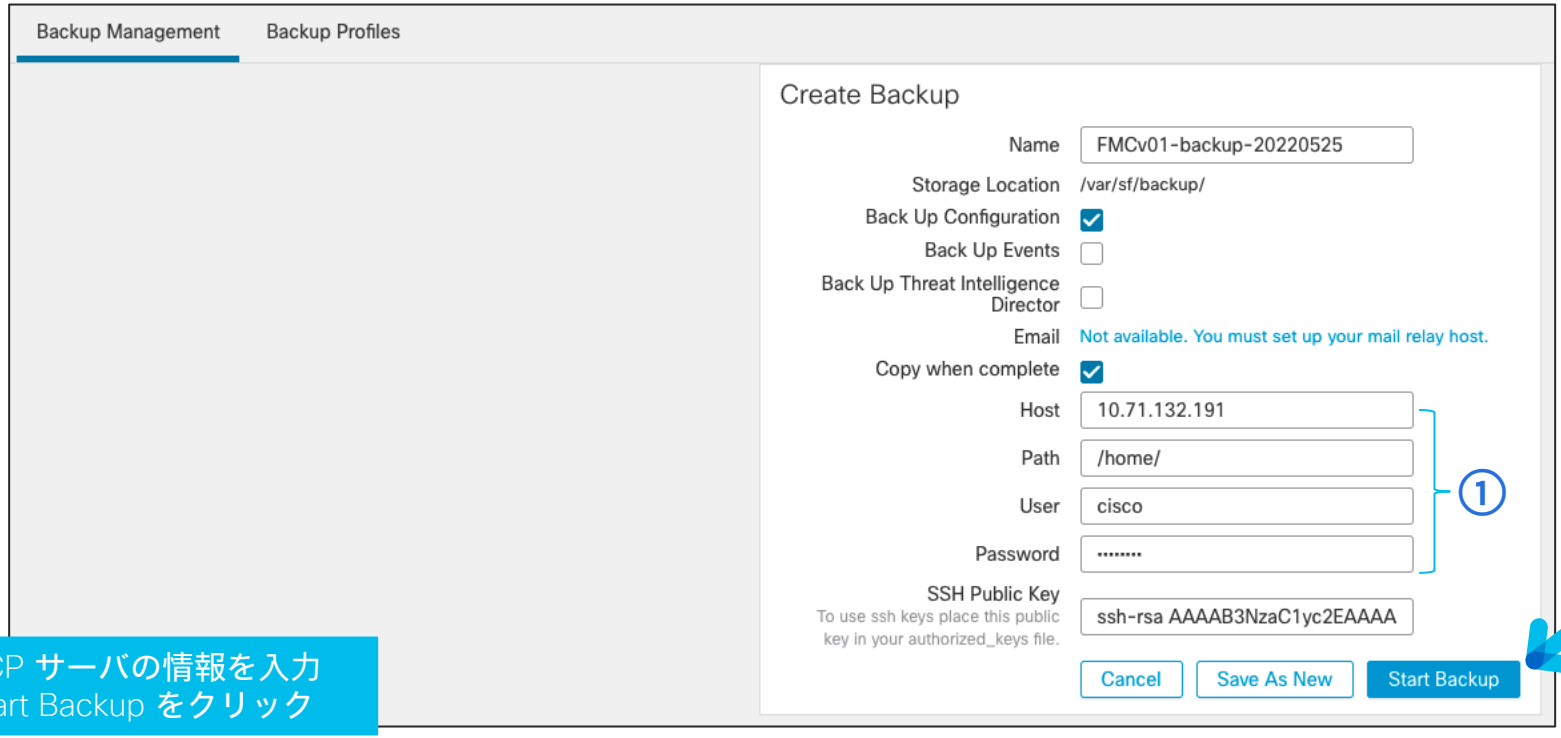
- バックアップ取得における各項目を設定



① バックアップの名前を入力、ここでは “FMCv01-backup-20220525” とする
② FMC の設定のバックアップを含める場合にチェックを入れる (デフォルト On)
③ イベントログや、Threat Intelligence Director のデータをバックアップに含める場合にチェックを入れる (デフォルト Off)
④ バックアップ取得後にメール通知を行う場合に設定
⑤ バックアップ完了後に SCP サーバへバックアップファイルをコピーする場合にチェックを入れる (デフォルト Off)

FMC のバックアップ取得 ③

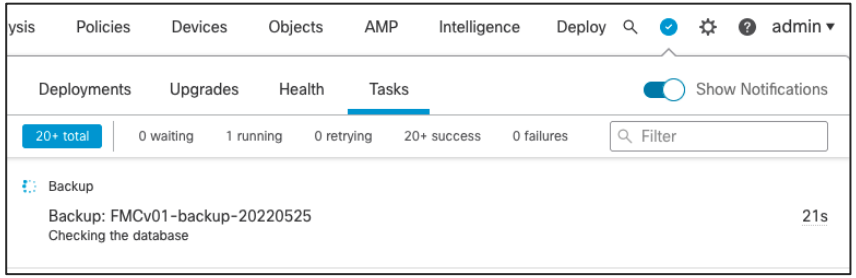
- バックアップファイルを SCP サーバへコピーする際に各項目を指定し、バックアップを開始

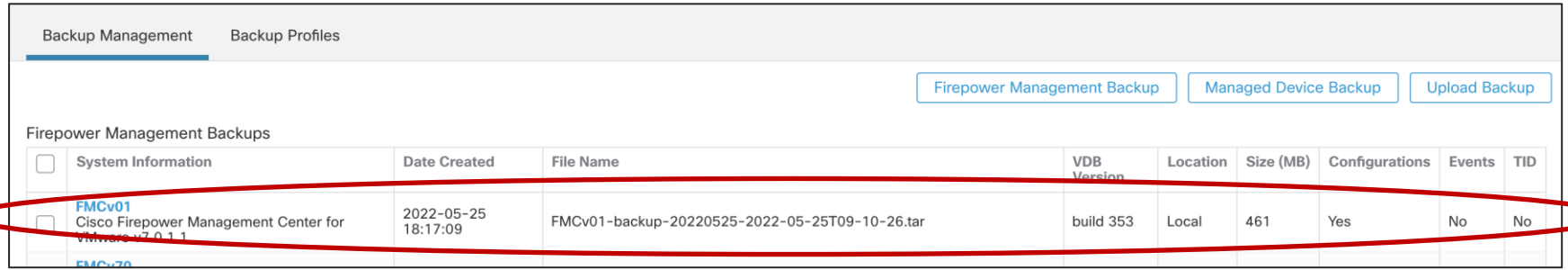


① SCP サーバの情報を入力
② Start Backup をクリック

FMC のバックアップ確認

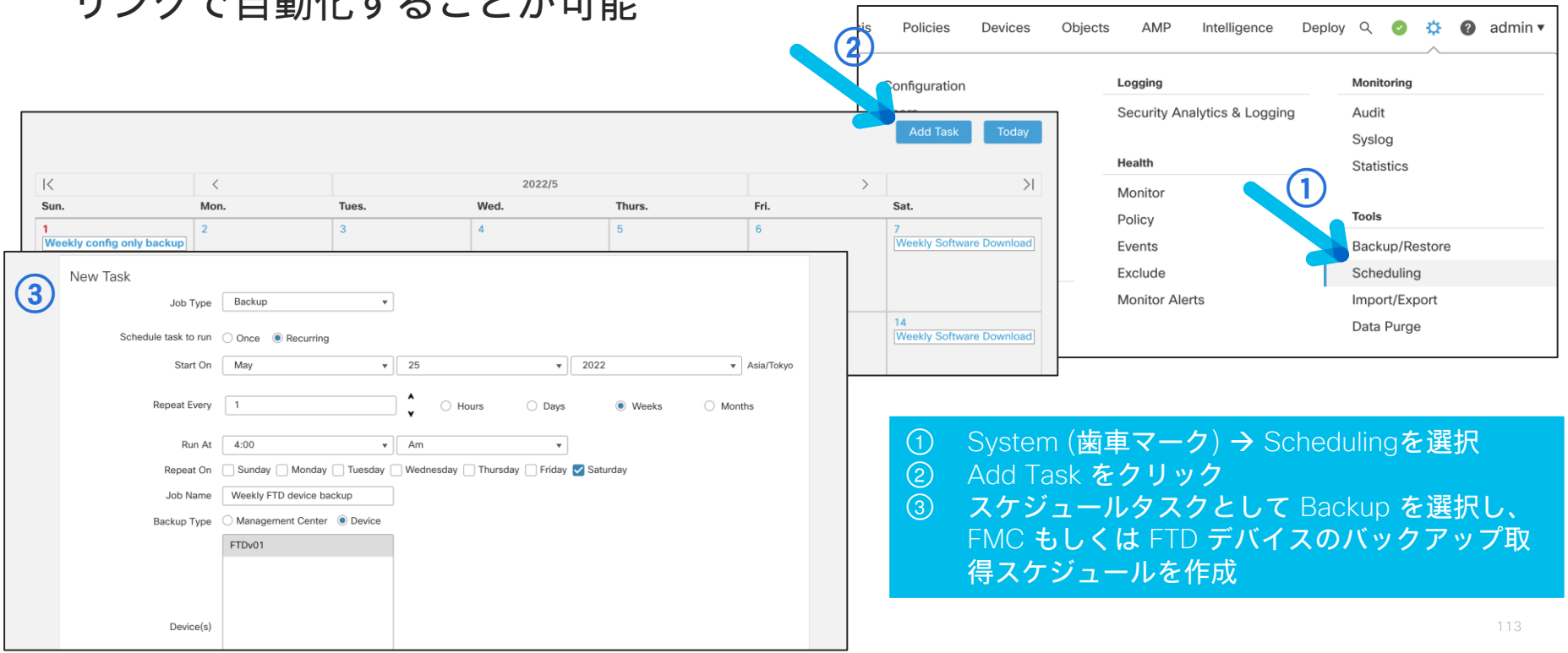
- バックアップ処理がスタートしたことを Task Tab (system の左隣) で確認
- 完了後に Backup Management のページの Firepower Management Backups にて、取得したバックアップファイルの存在を確認





参考: スケジューリングバックアップ

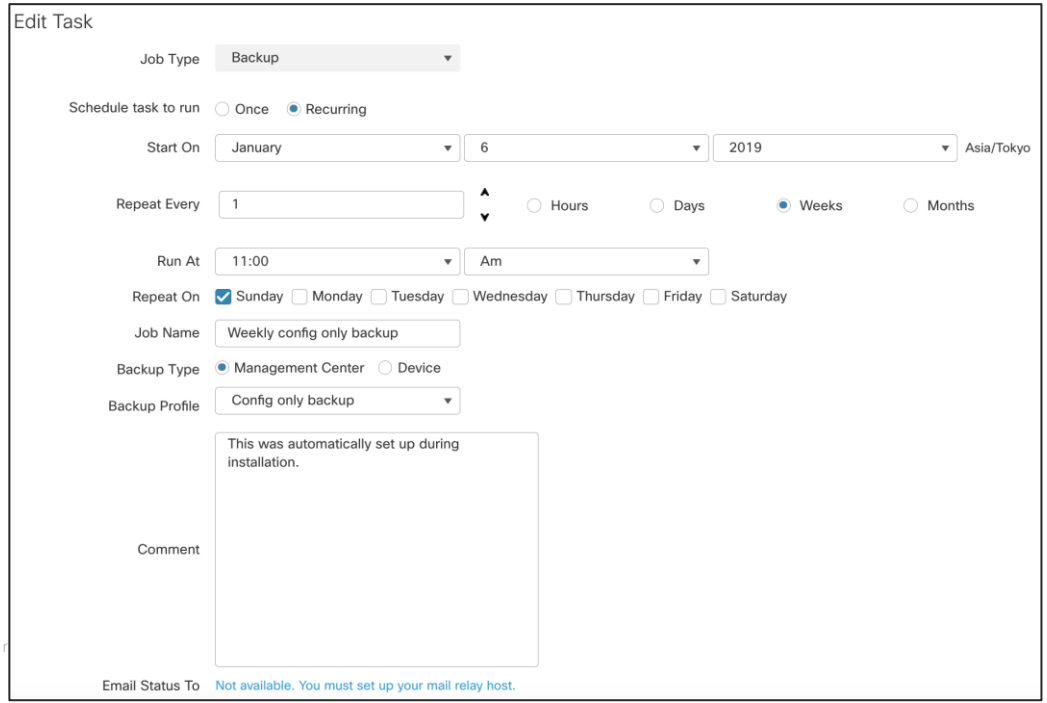
- FMC にて、FMC 自身および FTD デバイスのバックアップ取得を、スケジューリングで自動化することが可能



① System (歯車マーク) → Schedulingを選択
② Add Task をクリック
③ スケジュールタスクとして Backup を選択し、FMC もしくは FTD デバイスのバックアップ取得スケジュールを作成

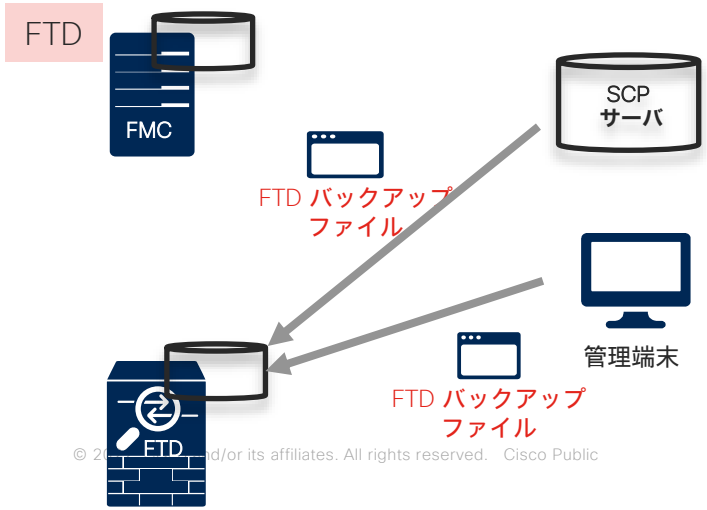
参考: FMC バックアップスケジューリングタスクの自動生成

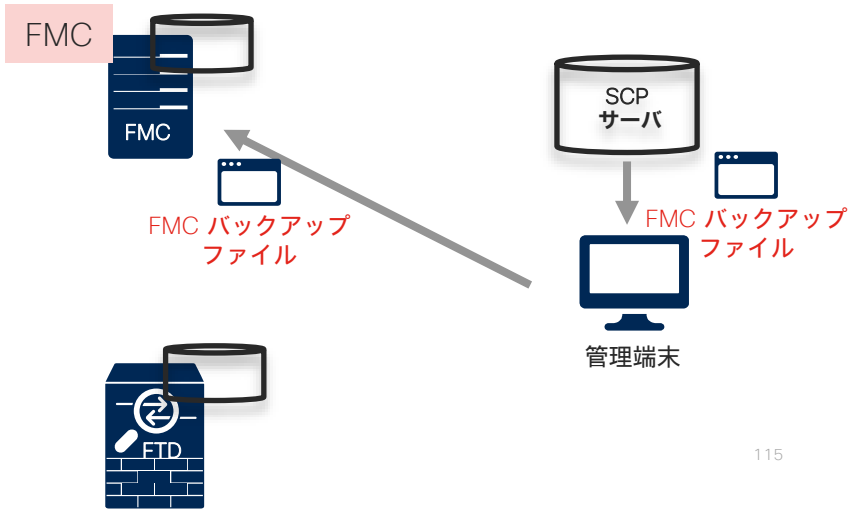
- FMC を新規にインストールした場合には、FMC 自身のバックアップ取得をウイークリーで実施するように、タスクが自動的に作成される



リストアについて

- FTD リストアは、取得済みのバックアップファイルを SCP サーバ、もしくは FTD ローカルにアップロードして実施
- FMC リストアは、取得済みのバックアップファイルを FMC ローカルにアップロードして実施
- FMC, FTD ともにリストア時にはバックアップ取得時のソフトウェアはパッチレベルまで同一にしておく必要がある
- FTD リストア時にはさらに SRU, VDB も同一バージョンが必要 (FMC は不要)





本章のリストアに関する操作の流れ

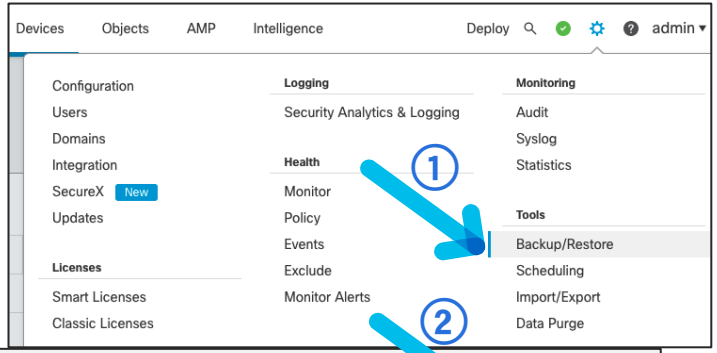
- FMC のバックアップファイルのアップロード
- FMC のリストア
- FTD デバイスのリストア (ローカルからのリストア)
- FTD デバイスのリストア (SCP サーバからのリストア)

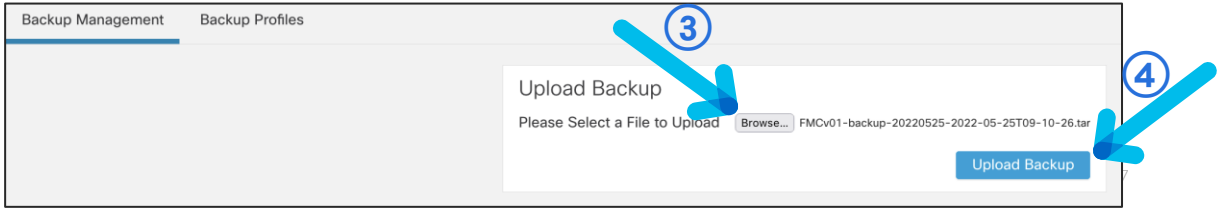
  - SCP サーバは、管理ネットワークに存在している PC を利用
  - FTD, FMC ともに HA でもリストアは可能

FMC のバックアップファイルのアップロード ①

- 機器交換等で、リストアに使用するバックアップファイルが FMC ローカルに存在しない場合には、取得済みの FMC バックアップファイルを、FMC ローカルにアップロード

① System (歯車マーク) → Backup/Restore を選択
② Upload Backup をクリック
③ Browse をクリックし、管理 PC に準備済みの FMC バックアップを指定
④ Upload Backup をクリックし、アップロードを開始

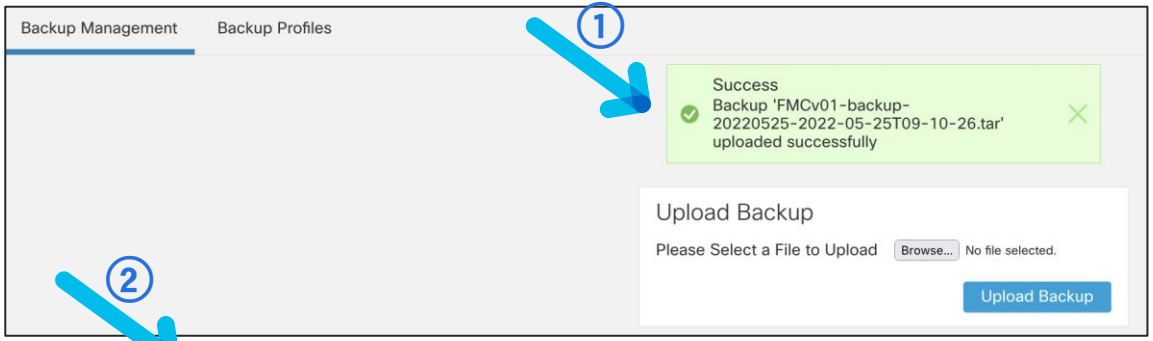


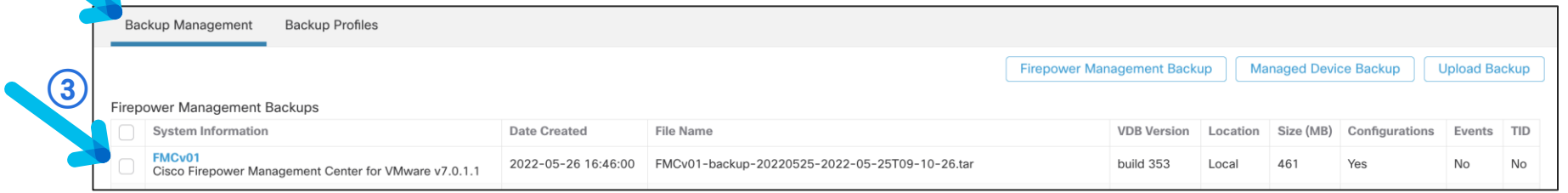


(注) リストア先の FMC は、バックアップを取得した FMC とソフトウェアバージョンとパッチを合わせて準備する。VDB や SRU はバックアップデータに含まれているバージョンで上書きされる

FMC のバックアップファイルのアップロード ②

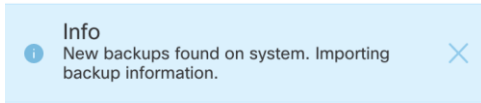
- アップロードした FMC のバックアップファイルが認識されていることを確認





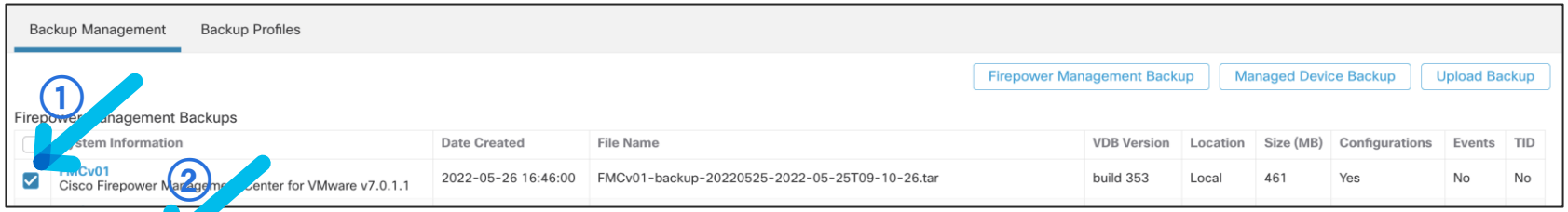
① アップロードが完了したメッセージを確認
② Backup Management をクリック (更新)
③ アップロードした FMC のバックアップファイルが認識されていることを確認

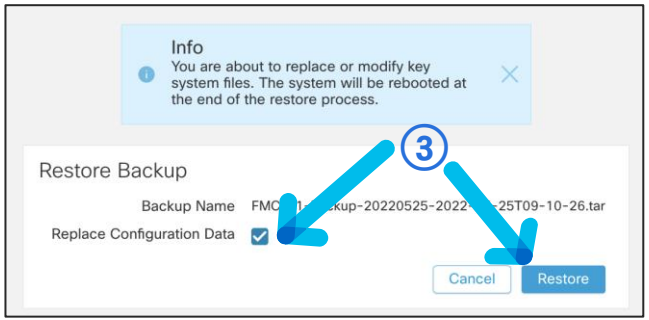
(注) アップロード直後に②を実施した場合、右のメッセージが表示され、ファイルが一覧に表示されないことがある。この場合は、まだ FMC がファイルに含まれている情報を読込中であるため、数分待って再度②を実施すること



FMC のリストア ①

- リストアに使用するバックアップファイルを選択し、リストアを実施

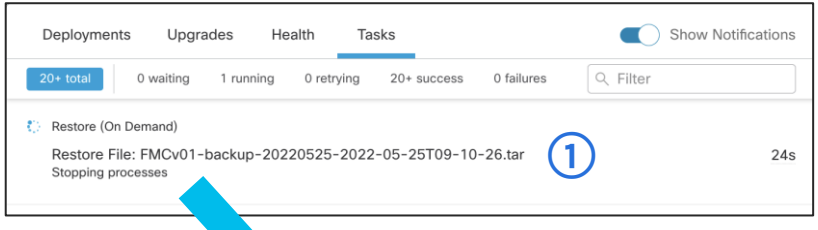




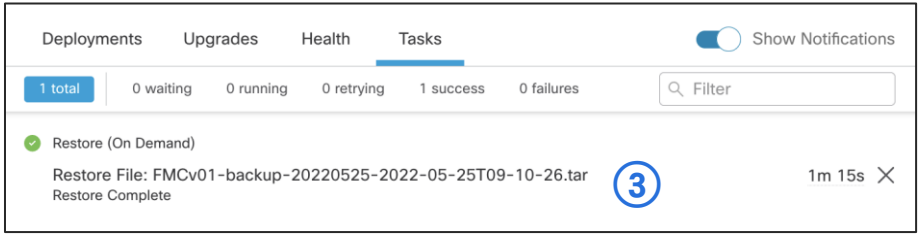
① リストアに使用する FMC のバックアップファイルをチェック
② Firepower Management Backups のファイル一覧の下にある Restore をクリック
③ Replace Configuration Data をチェックし、Restore をクリックしてリストアを開始

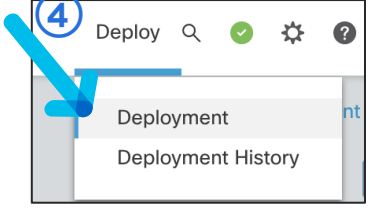
FMC のリストア ②

- リストアの途中で FMC が自動的に再起動する。再起動後、FMC にログインし、リストアが無事に終わったことを Task Tab で確認、その後 FTD デバイスに deploy を実施



②

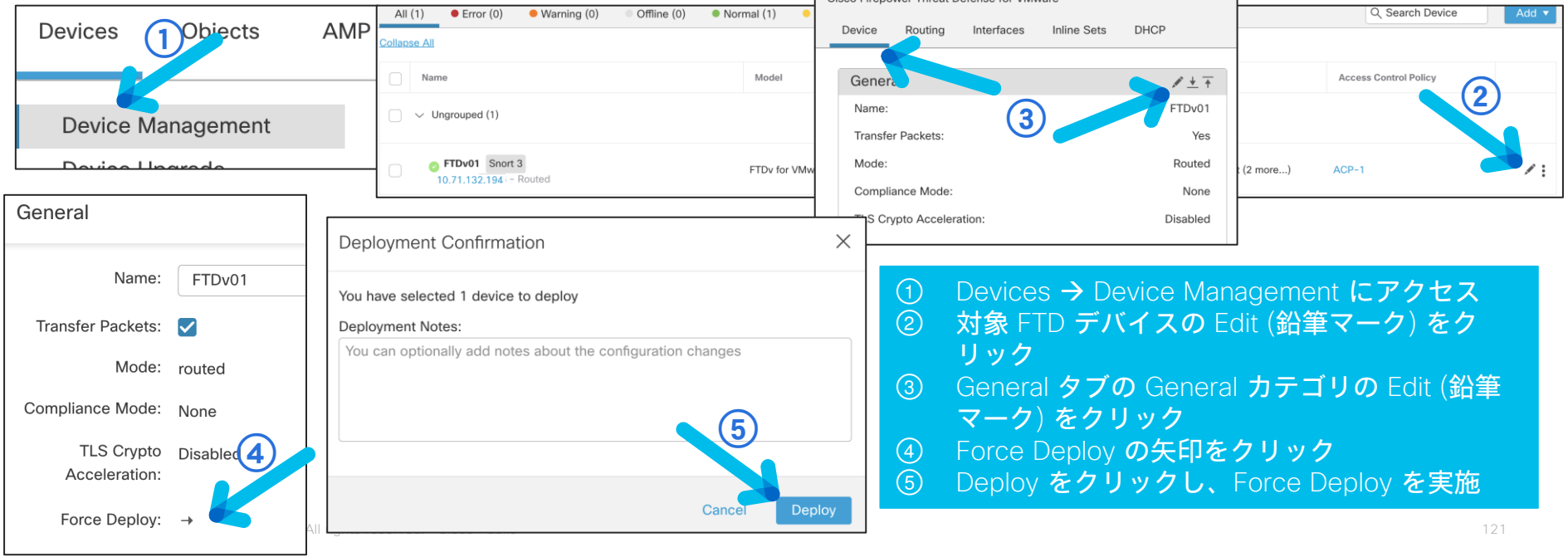




① リストア処理がスタートしたことをで確認
② 自動的に再起動した FMC にログイン
③ Task Tab で FMC のリストアが無事に終わったことを確認
④ FTD デバイスに deploy を実施

FMC のリストア ③

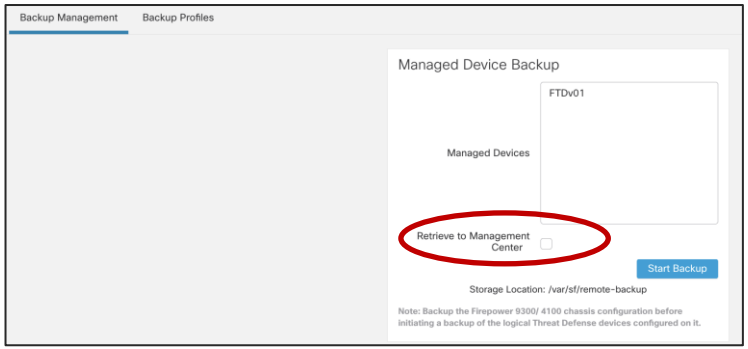
- もしも FTD デバイス up-to-date になっていた場合 (deploy が必要になっていない場合) は、Force Deploy の実施を推奨



① Devices → Device Management にアクセス
② 対象 FTD デバイスの Edit (鉛筆マーク) をクリック
③ General タブの General カテゴリの Edit (鉛筆マーク) をクリック
④ Force Deploy の矢印をクリック
⑤ Deploy をクリックし、Force Deploy を実施

FTD デバイスのリストア (ローカル) ①

- FTD のバックアップを取得する際に、Retrieve to Management Center にチェックをいれていなければ、FTD の /var/sf/backup/ にバックアップファイルが保存されている。この場合には、そのファイルを利用してリストアが可能




```
> expert
admin@FTDv70-1:~$ cd /var/sf/backup/
admin@FTDv70-1:/var/sf/backup$ ls -atl
total 122780
drwxr-xr-x  2 www  www       4096 May 26 08:35 .
-rw-r--r--  1 www  root 125716480 May 26 08:35 FTDv01_20220526173126.tar
drwxr-xr-x 77 root root      4096 May 25 07:20 ..
```

FTD コンソールの expert モードでバックアップファイルの存在を確認可能

(注) リストア先の FTD は、バックアップを取得した FTD とソフトウェアバージョンとパッチ、および VDB や SRU を合わせて準備する必要あり

FTD デバイスのリストア (ローカル) ②

- FTD の CLISH (コンソール) でリストアコマンドを実行、バックアップファイルの詳細を確認

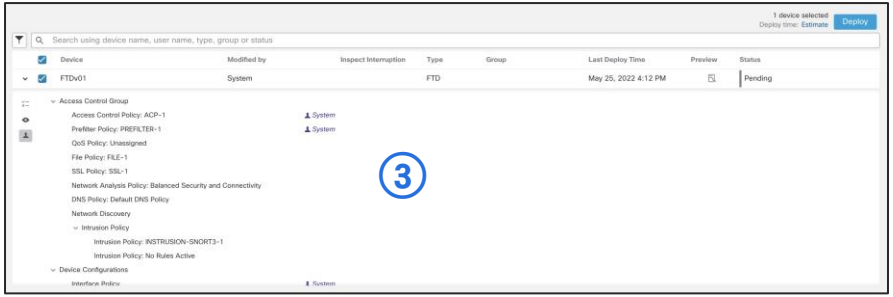
```
> restore remote-manager-backup FTDv01_20220526173126.tar

Device model from backup :: Cisco Firepower Threat Defense for
VMware
This Device Model  :: Cisco Firepower Threat Defense for VMware

********************************************
          Backup Details
********************************************
Model = Cisco Firepower Threat Defense for VMware
Software Version = 7.0.1.1
Serial = 9AR5P6F3V0F
Hostname = FTDv70-1
Device Name = FTDv01
IP Address = 10.71.153.76
VDB Version = 353
SRU Version =
Manager IP(s) = 10.71.132.200
Backup Date = 2022-05-26 17:31:26
Backup Filename = FTDv01_20220526173126.tar
********************************************
```

① restore コマンドを FTD の CLISH で実施
② バックアップファイルに含まれる情報を確認

FTD デバイスのリストア (ローカル) ③

- バックアップファイルの内容に問題がなければ、リストアを開始。FTD デバイスは自動的に再起動する。再起動後は FMC から deploy を実施、もしも FTD デバイスが up-to-date であれば、Force Deploy を推奨

```
********************* Caution ****************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches
versions from backup manifest before proceeding.(Running 'show
version' command on FTD, displays Model Name and version details).
Restore operation will overwrite all configurations on this device with
configurations in backup.
If this restoration is being performed on an RMA device then ensure old
device is removed from network or powered off completely prior to
proceeding with backup restore.
 ************************************************************

Are you sure you want to continue (Y/N) y        ①
Restoring device . . . . . .
②
```



① バックアップファイルの内容に問題がなければ y を入力してリストアを開始
② FTD へのリストアが実施され、FTD デバイスが自動的に再起動
③ FTD デバイスへの deploy を FMC から実施

(注) FTD デバイスへの Force Deploy 方法は FMC のリストア時と同じ

FTD デバイスのリストア (リモート SCP) ①

- FTD デバイス交換時等で FTD デバイスのローカルにバックアップファイルが無くても、SCP サーバに FTD デバイスのバックアップファイルがあれば、それを直接指定して CLISH (コンソール) でリストアコマンドの実行が可能、あとはローカルからのリストアと同じ

```
> restore remote-manager-backup location 10.71.132.191 cisco /home/ FTDv01_20220525154627.tar
Enter SCP password:

Device model from backup :: Cisco Firepower Threat Defense for VMware
This Device Model  :: Cisco Firepower Threat Defense for VMware

***********************************************
        Backup Details
***********************************************
Model = Cisco Firepower Threat Defense for VMware
Software Version = 7.0.1.1
Serial = 9AR5P6F3V0F
Hostname = FTDv70-1
Device Name = FTDv01
IP Address = 10.71.153.76
VDB Version = 353
SRU Version =
Manager IP(s) = 10.71.132.200
Backup Date = 2022-05-25 15:46:27
Backup Filename = FTDv01_20220525154627.tar
***********************************************
```

① restore コマンドを FTD の CLISH で実施、引数に SCP サーバの IP アドレスやユーザ名、パス、ファイル名を指定
② SCP サーバにログインするパスワードを入力
③ バックアップファイルに含まれる情報を確認

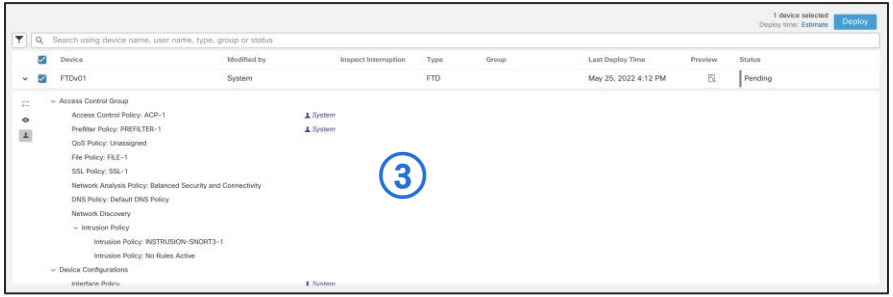
(注) リストア先の FTD は、バックアップを取得した FTD とソフトウェアバージョンとパッチ、および VDB や SRU を合わせて準備する必要あり

FTD デバイスのリストア (リモート SCP) ②

- バックアップファイルの内容に問題がなければ、リストアを開始。FTD デバイスは自動的に再起動する。再起動後は FMC から deploy を実施、もしも FTD デバイスが up-to-date であれば、Force Deploy を推奨

```
********************* Caution ****************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches
versions from backup manifest before proceeding.(Running 'show
version' command on FTD, displays Model Name and version details).
Restore operation will overwrite all configurations on this device with
configurations in backup.
If this restoration is being performed on an RMA device then ensure old
device is removed from network or powered off completely prior to
proceeding with backup restore.
 ************************************************************

Are you sure you want to continue (Y/N) y
Restoring device . . . . . .
```

① ②



① バックアップファイルの内容に問題がなければ y を入力してリストアを開始
② FTD へのリストアが実施され、FTD デバイスが自動的に再起動
③ FTD デバイスへの deploy を FMC から実施

(注) FTD デバイスへの Force Deploy 方法は FMC のリストア時と同じ

The bridge to possible